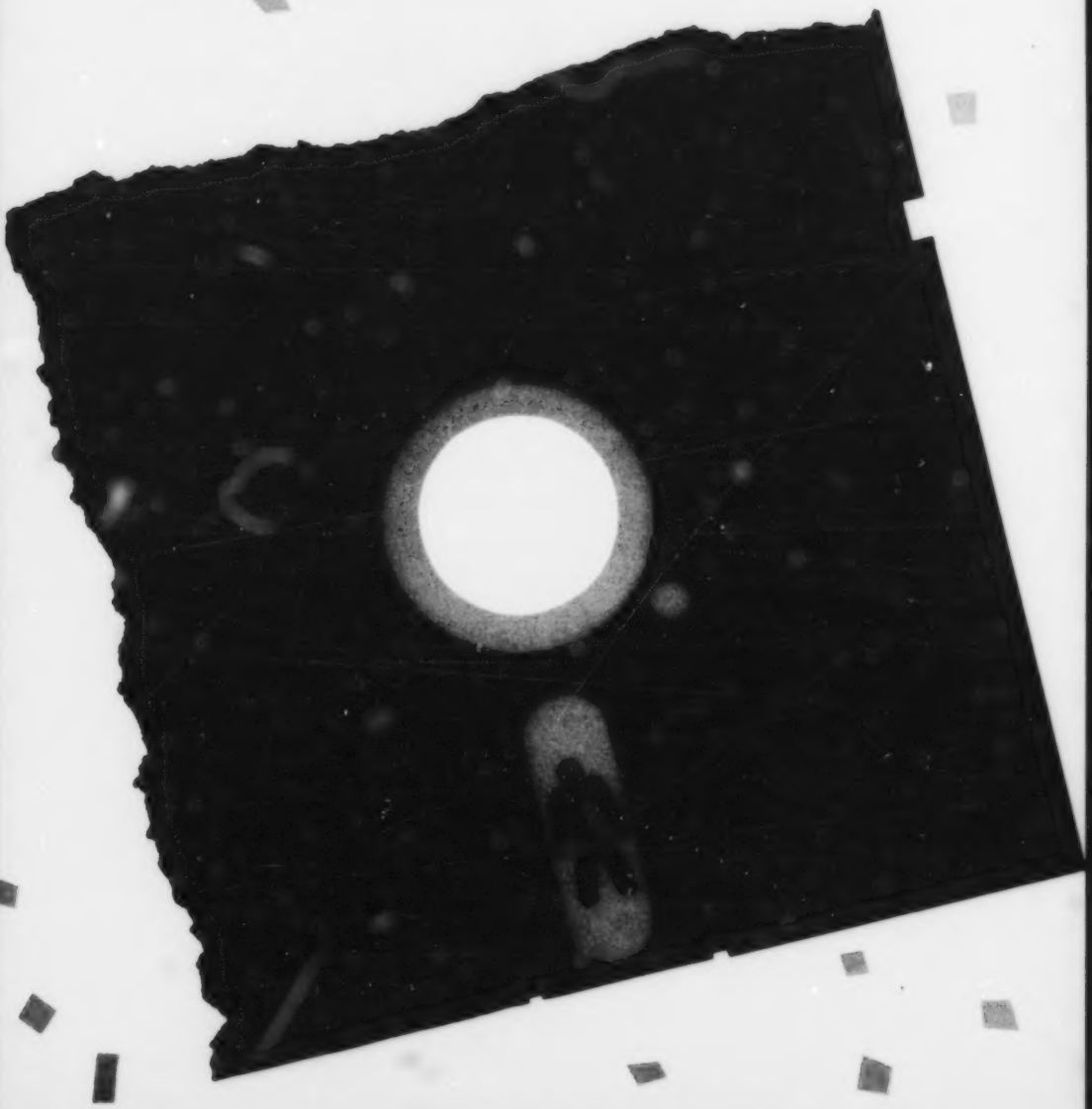
Privacy Commissioner

Annual Report 1989-90



Annual Report
Privacy Commissioner
1989-90

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501

© Minister of Supply and Services Canada 1990

Cat. No. IP30-1/1990

ISBN 0-662-57525-3

90-06898/

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

May 22, 1990

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1989 to March 31, 1990.

Yours sincerely,

John W. Grace

John W. Grace
Privacy Commissioner

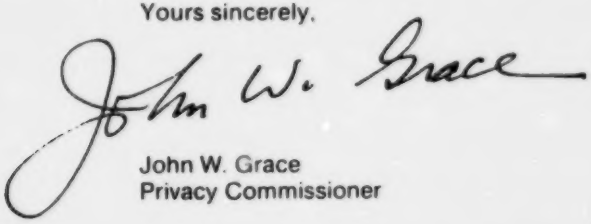
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

May 22, 1990

Dear Mr. Fraser,

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1989 to March 31, 1990.

Yours sincerely,



John W. Grace
Privacy Commissioner

Table of Contents

Mandate 1
The Sermon: An end of term report 2

During the Year 16
Public servants' hot line 16
Reviewing the CSIS act 17
SINning...again 19
Thanks to Mr. Statsman 20
Spreading the word 21
Drug testing—everybody's doing it 22
Genetic analysis 23
Police databases—CPIC 24
Ring, ring...Orwell calling 26
A new exempt bank 27

Complaints Directorate 29
Data-matching review 31
Notifying the Commissioner 33
Some cases 36
Inquiries 50

Compliance Directorate 52
A seven-year retrospective 52
What was found 54
Some incident investigations 56

Corporate Management 57

Appendices 59
I Organization chart 59
II Government institutions covered by the Act 60

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to:

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible; and
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness

Individuals in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the Personal Information Index description of the contents of the information bank is deficient in some way;
- the department's listing in the Index does not describe all the uses it makes of personal information;
- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

The Sermon

"The future is not what it used to be."
—William McNeill, Professor of History Emeritus, University of Chicago.

An end-of-term report

An end-of-term report offers a once-in-seven-year opportunity to range beyond the arbitrary confines of 12 months in appraising the privacy state of the nation. Of course, there is some grandiosity (or threat?) to that promise. The *Privacy Act* requires, after all, only an annual accounting to Parliament and the legislation covers only the federal government, not the country.

Yet comments based upon seven years of observing privacy protection (or lack of it) should be better grounded than those based on the experience of the last 12 months. If the observations and judgments in this report sometimes reach beyond the narrow legal confines of the *Privacy Act*, that itself is because a privacy commissioner's office by 1990 has inevitably been drawn into the day's larger and newly-emerging privacy issues.

That does not mean that a privacy commissioner should try to impose his writ upon areas where he has no jurisdiction. But to stay out of the fray and ignore the privacy aspects of, say, AIDS or drug testing—two momentous issues of our time—would be to risk irrelevance and to preside over the diminishment of the office. Perhaps the most encouraging development in seven years has been the way in which the office of the Privacy Commissioner, like it or not and justified or not, has been used as a national privacy resource centre.

Inquiries from the public have increased from 1008 in 1984-85 to 3447 in 1989-90. The subject of the calls and letters range from queries on when a Social Insurance Number must be given (still the most frequent question) to media requests for comment on matters with potential privacy implications; from telephone gadgetry showing a caller's telephone number on a screen to an Auditor General's proposal for an anonymous fraud hot line to a proposal by a municipal council to circulate detailed profiles of released offenders.

Privacy moved from a peripheral social issue, from being a rather esoteric, rarefied—almost cult—concern into the main stream of public consciousness. That is the positive change of the past seven years, and the awareness continues to grow.

The awareness grows with each new intrusion upon private lives by the information society—and the information economy. Turning to privacy values is an instinctive human response to, and defence against, a prying, pervasive technology. The cry for privacy protection is a plea that human values—human dignity—should prevail against a computer-driven culture which would claim sovereignty over every recorded transaction. It is sometimes argued the massive information storage and retrieval capacities of the computer make possible a new Renaissance of learning, an age when machines can do what men could not do without unimaginable drudgery—and perhaps not even then. Comfort has been taken in the notion, as one commentator has put it, that "information is a renewable resource".

Unlike trees or oil, information can indeed be renewed: better computers linked to better communications systems can renew—and expand—information almost to infinity. But human privacy is not renewable. There's the rub. Once lost to an indiscreet computer, a person's privacy is gone forever. The computer never forgets.

In a laissez-faire information society, there is no control even over the uses of one's own name. As the American attorney and communications scholar Anne Branscomb has written, the only way to stop the trafficking in a person's personal information is to "become a hermit, have an unlisted telephone, never charge anything and stop buying any items from catalogues". Even such unnatural precautions may offer no real guarantee.

The consciences of the collectors of personal information are all that control the uses of private-sector databases. Voluntary codes of fair information practices are visible evidence of ethical intent. Here there is some reason for encouragement, as is discussed later. But should one choose not to share one's own information with the marketplace, there is negligible legal protection in the now open season on personal information.

The dark side

Too many Canadians continue to remain unaware of the *Privacy Act* and the important rights it confers. The fact that 3[illegible],000 individuals have used the Act to apply for their information in federal government files shows, however, that the legislation is becoming better known and, when known, it is used. More and more Canadians are increasingly, if vaguely, aware of the dark side of new technologies which can transform persons into "data subjects" and develop profiles of greater or lesser accuracy based upon personal information winkled out of proliferating data bases.

These gloomy observations are not simply the subjective judgment of a professional privacy advocate. Public opinion poll after another show that protection of privacy ranks high among the most pressing issues facing modern society.

What chance does privacy have when satellites can conduct surveillance from more than 300 kilometres in the sky? Audio eavesdropping no longer demands physical access to a building in order to plant listening devices. And, of course, most of us carry in our wallets or purses the key to vast amounts of highly sensitive personal information. Our ubiquitous bank and credit cards leave a trail of where we travel, eat, shop and sleep—perhaps by matching records—even with whom! George Orwell could not have imagined the new possibilities of Big Brother.

Professor David Flaherty of the University of Western Ontario is an internationally recognized authority on data protection. He served as consultant to the Justice and Solicitor General Committee's review of the *Privacy Act* and he has been quoted before in these reports. His recent book, called *Protecting Privacy in Surveillance Societies* (University of North Carolina Press), argues with chilling persuasiveness that individuals "are increasingly subject to surveillance through the uses of data bases in the public and private sectors and that these developments have negative implications for the quality of life in our societies and for the protection of human rights."

What can be left of the right to be left alone (and courts are defining precisely such a right), he asks, when credit bureaus monitor the credit information of millions of Canadians and the names of perhaps 10 per cent of this country's adult population may be contained in the national police computer known as the Canadian Police Information Centre?

Add to these, burgeoning federal and provincial government data bases holding personal data of greater or lesser sensitivity on everyone who has ever breathed the air of the country. Seven years ago, the federal government held, on average, 10 to 12 files on each person in Canada. Today, the number is closer to 20. The sheer magnitude of such data bases goes a long way to demonstrate Professor Flaherty's thesis that western industrial societies run the increasing risk of becoming, if they are not already, surveillance societies.

"There has to be some consideration for individual rights. We can't be running around testing anybody at any time."
—Pat Bowlen, owner of the Denver Broncos.

Privacy and the Charter

There is, however, some room for encouragement, though certainly not smugness, in the knowledge that Canadians are better defended against uncontrolled surveillance than other societies. In addition to the protection and rights provided by the *Privacy Act*, the *Charter of Rights and Freedoms* is proving to be an unexpected and surprisingly effective defender of privacy values.

Privacy is not mentioned as a specific right guaranteed by the Charter. Yet the Supreme Court of Canada has interpreted sections of the Charter unambiguously and vigorously as statements of privacy protection. Attention has been called in earlier of these reports to previous Supreme Court decisions which established that the "right to be secure against unreasonable search and seizure" (section 8 of the Charter) protected individuals from unjustified intrusions upon their privacy. On January 25 this year, in *Mario Duarte v. Her Majesty The Queen*, that reading of the Charter was spectacularly re-affirmed in the decision concurred in by six of seven Justices.

The case turned on whether it was legal, under the Charter, for the police to have an informer record, surreptitiously and without a judicial warrant, his conversation with a suspected drug dealer. The Supreme Court of Ontario had held that the police (though not private citizens) were free, without judicial warrant, to "bug" private conversations as long as they had the co-operation of one of the parties.

In writing for the majority, Mr. Justice La Forest built upon the Supreme Court's earlier decisions (his own among them) that "the primary value served by section 8 of the Charter is privacy". The following paragraph should end any doubt of how effectively the Court and the Charter can respond to technology threats to personal privacy:

> "The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made every time we opened our mouths might be superbly equipped to fight crime, but it would be one in which privacy no longer had any meaning".

The importance of this judgment can hardly be over-estimated and it is deserving of more attention than it has received.

The good news is that the case lays down rules restricting the use of electronic surveillance by police authorities. The Supreme Court decision makes the country at least a more private place than it might have been.

The *Criminal Code*, however, does not prevent private citizens from intercepting the conversations of others as long as one of the parties to the conversation consents. Through this loophole the surreptitious use of microphones hidden in briefcases and umbrellas, parabolic dishes and the widely-advertised "whisper 2000" directional microphones continue to proliferate.

The criminal law should make the surreptitious interception of all private communications unlawful by requiring the consent of all parties to the communication to any recording or interception.

"When a reporter enters the room, your privacy ends, and his freedom begins."
—Warren Beatty.

Privacy and the media

Another recent Supreme Court judgment compels equal attention.

In this case, *Edmonton Journal v. Alberta*, a majority of the Court held that intrusions upon the personal privacy of individuals were justified by the higher public good in the freedom of the press to report court cases.

But the dissent of Mr. Justice La Forest, writing for Madame Justice L'Heureux-Dubé and Mr. Justice Sopinka was, for a privacy advocate, more significant than the view of the majority. Earlier Court decisions placed limitations upon *governmental* intrusions; the dissent would protect individual privacy from assault from non-governmental sources. In this case, Mr. Justice La Forest was willing to extend the Court's protection because, he wrote, "in our society the privacy of the individual is as often threatened by other powerful or influential entities against which the individual is powerless".

Other entities, indeed. Three Supreme Court Justices concurred in the following: "The protection from intrusion on the privacy of the individual, the family and witnesses...in itself affords a sufficiently compelling objective to warrant some curtailment of the freedom of the press in the present context." (The context was a matrimonial dispute.)

No state secrets here to protect. No threat to the privacy of ordinary citizens from government. In an almost trivial matter, so far as the state is concerned, the minority was ready to extend existing prohibitions upon publishing personal information. They would go considerably beyond restrictions pertaining to victims of assault or to young offenders. The dissenting judges were willing to place new limits upon press freedom because the disclosure "of personal information about an individual by the mass media can do incalculable harm to the individual and his/her family".

The view of the majority, which held that there should be no restrictions placed upon the reporting of matrimonial cases, has received all the media attention. The dissent has been all but ignored. In the long term, however, it may be shown that the balance, that anguishingly difficult balance, between privacy and press rights which has been struck in the *Edmonton Journal* case is not good enough. It will need fine tuning and Mr. Justice La Forest, Mr. Justice Sopinka and Madame Justice L'Heureux-Dubé may yet be proved right.

The threats posed in this case to a free press were, after all, theoretical. The invalidated law respected the principle of open courts. Access by those having serious interest in court proceedings or family law is permitted. All the general information about the nature of the case may be published. Moreover, the *Edmonton Journal* presented no evidence that, throughout its 50 years, there was a single instance where the rejected provision forbade it from reporting on a matter of public interest.

Little wonder that the dissenting judges expressed scepticism of the significance of the negative impact of the legislation on freedom of the press and media, and the public's right to be informed of matters of public interest.

But, on the other side, the harm is real and present.

In Justice La Forest's words:

> "In matrimonial cases, the individual is forced to reveal many aspects of his or her private life in order to comply with the demands of the state in ordering his or her life. This necessary intrusion on family privacy, we saw, may have serious impact not only on the litigants themselves but on witnesses and, even more important, children."

The far greater threat to freedom of the press today comes from some of the media's own excesses in intruding, shamelessly and aggressively, into private lives in matters where there is no public interest, only public curiosity or, even, prurience. In the United Kingdom, a reaction to such excess brought about the introduction of legislation which would have restricted, in the name of privacy protection, the publication of personal information. That legislation has been withdrawn, wisely; it was dangerously drafted. But the fact that it was a near thing in Britain—and the closeness of the Supreme Court's decision in Canada—should cause the media to examine their collective conscience (is there such a thing?), if only from the point of view of enlightened self-interest.

Justice La Forest's observation that "privacy ranks high in the hierarchy of values meriting protection in a free and democratic society" is a message more than an aphorism. The message is that privacy is a value which the courts—and the public—may be increasingly willing to place higher than even that of a free press.

Real progress

If there is truth to the proposition that Canada is doing better than most societies in holding back the intrusions of the new, aggressive technologies which would treat human beings as mere data subjects, the credit must not only go to a vigilant Supreme Court, but to Parliament and, yes, the government.

The most significant privacy happenings in the past seven years were, perhaps in this order, the review of the *Privacy Act* by the Justice and Solicitor General Committee, the government's generally positive response to that committee's recommendations in *The Steps Ahead* and two government policy initiatives: the first, reining in the Social Insurance Number (the now infamous SIN), the second, imposing controls over computer matching or linkage.

These achievements have been commended in earlier reports and must be singled out again in this retrospective. Without the enthusiastic and unanimous re-affirmation of the *Privacy Act* by the Parliamentary committee and the government's acceptance of the committee's principal recommendations, atrophy might have set in.

It was enormously important that the Parliamentary review found that the *Privacy Act* had struck the proper balance between the public interest and private rights. There had been some scepticism from both sides—from chiefs of police and civil libertarians—over that balance. Parliament must have had it right because, on review, not a whimper of complaint was heard from either side of the ideological barrier.

"...aspiring bureaucrats are constantly inventing new ways to use existing data for other administrative purposes.'

David Flaherty, Protecting Privacy in Surveillance Societies.

As a result of support from the top, privacy as an issue in Canada has developed considerably beyond awareness, however necessary that is for the beginning of reform. Seven years ago, privacy rights and the need for privacy protection remained largely abstractions. Today the talk is of specifics: bringing the use of the Social Insurance Number under better control (Why do banks demand a SIN? Must I give my SIN in opening a new account?); controlling the use of compulsory tests in the search for the "perfect" employee; limiting the traffic in personal information that reveals individual's spending choices—from goods purchased to charity donations; and questioning the intrusiveness of market surveys, political polling, and census-taking (Do they ask too much and what do they do with the information?).

Even those who are not computer literate are aware of the ability of small and cheap computers to mix, match and massage data bases. Techno-peasants, data protectors included, are aware of the downside of efficiency. The claimed benefits from linkages (tracking down cheaters or debtors, for example) may come at the unacceptable cost of systematic population monitoring. In Canada, computer matching by federal government institutions is now covered by strict rules under which the Privacy Commissioner's office plays a role. The Americans have even encased their matching controls in federal legislation.

"We are travelling in the fast lane without side-view or rear-view mirrors."
—Henry Wiseman, Chairman, World Conference on Ethics and Technology, University of Guelph.

The "what" act?

Little has been static in the privacy business these past seven years, neither the threats nor the responses. The impact of the *Privacy Act* upon the public, the government and the public service is now irreversible. As noted earlier, by the end of seven years almost 300,000 individuals (the count is Treasury Board's, not the Privacy Commissioner's) will have used the *Privacy Act* to apply formally for their personal information held by the government. That is a surprising figure. What would the numbers be if the *Privacy Act* were more widely-known?

After all the speeches and reports by the Privacy Commissioner, not enough Canadians are aware of their privacy rights. Even public servants remain unaware both of their own rights and responsibilities under the legislation. The latter is not a subjective judgment: it is the most common single finding of the office's privacy auditing.

Yet ask any senior public service manager (or any public servant aspiring to be a senior manager) and he or she will be as aware of the *Privacy Act*, well, almost, as the *Official Languages Act*. Privacy is now part of the public service's psyche.

Note these three important initiatives in the past year alone:

Item: National Defence now gives members of the Canadian Forces access to their current evaluations and to their position on a merit list without a formal request under the *Privacy Act*.

Item: Supply and Services put in place a strict policy ensuring that government mailings comply with the *Privacy Act*. On its part, Treasury Board has published guidelines to all departments covering uses of their mailing lists.

Item: Employment and Immigration, Industry Science and Technology, the Canadian Security Intelligence Service, among others, conduct their own internal audits to determine compliance with the *Privacy Act*.

On the most senior levels, there is now an ethos of acceptance of and respect for privacy principles. The most striking reason for this perhaps surprising generalization is that in seven years the Privacy Commissioner has not been forced to his ultimate resort—to bring a case against a government institution before the Federal Court. There have been a few, but only a few, settlements at the court house door. The crucial point is that in the crunch no recommendation of the Privacy Commissioner has been defied.

Of course, the reason Parliament put a privacy ombudsman in place was precisely to negotiate disputes and avoid recourse to the courts. The courts would be the first to say that they are overburdened enough without being asked to settle privacy quarrels.

It is not unseemly to boast of that non-court record because it takes two to tango. In this end-of-term reckoning, nothing is more important for the Privacy Commissioner to do than to commend ministers, deputy ministers, privacy coordinators and managers alike for their sensitivity to the letter and spirit of the legislation.

The willingness to make the *Privacy Act* work has been demonstrated across the board: from the Royal Canadian Mounted Police and the Canadian Security and Intelligence Service, the holders of some of the most sensitive personal information, to Employment and Immigration Canada and Revenue Canada, the custodians of the largest holdings of information, to the smallest, the Yukon Territories Water Board with (at last count), its three files.

The coordinators...still

As important as court cases which didn't happen (and another reason for that) is the increasingly close rapport achieved over the years between departmental privacy coordinators and investigators from the Privacy Commissioner's office. The busiest privacy coordinators are now as expert in at least some aspects of the *Privacy Act* as privacy investigators. They share a growing body of knowledge and precedents; their expertise enhances their value to their own institutions, especially as cases become more complex.

Coordinators have in fact emerged, albeit mainly in larger institutions, as privacy professionals. Theirs is not an easy role, caught between natural loyalties to a department and to the *Privacy Act*. Sometimes the role calls for heroism.

Enlightened departments now give their coordinators the status the job deserves. Last year, the coordinator for Veterans Affairs conducted briefings at regional departmental offices across the country. Her teaching role (with a travel budget of $17,000), was tangible testimony to her department's commitment to the *Privacy Act*.

"and miles to go..."

So much for the credit side of the ledger.

A balance sheet must also report debits, some of which run deeper than even that most spectacular of privacy breaches—that privacy Chernobyl—the theft of the tax information of some 16 million Canadians from a Toronto office of Revenue Canada. That incident more widely brought home the vulnerability of data holdings and showed the need for data protection than all the preachments of a privacy commissioner.

Yet, even after all the good things are said, too many rank-and-file federal public servants, as noted earlier, remain in blissful ignorance of privacy rights and privacy responsibilities. After seven years, there shouldn't be a federal government employee unaware of the *Privacy Act*. Yet each privacy audit by compliance investigators turns up the same dreary chronicle of pervading ignorance, not among senior managers, but at levels where it is by now inexcusable. This past year has seen Treasury Board privacy courses given to some 700 public servants. That is an important beginning—but only a beginning.

"To avert disaster we have not only to teach men to make things, but also to produce people who have complete control over the things they make."
—Prince Charles.

Unfortunately, an important component of any training—audio-visual material—is still missing. Both Treasury Board and the Commissioner's office make do with tapes of items aired on commercial TV. After seven years it is frustrating, and not a little embarrassing, to have to refer federal institutions to the Ontario and Quebec provincial commissioners for training audio-visuals. In fact, the office's 1990 request for a modest $70,000 for public affairs was turned down because, with its heavy complaint load, the office "is well enough known".

There is better excuse for other Canadians to be unacquainted with the *Privacy Act*. The Treasury Board and the Privacy Commissioner's office have had only modest resources to engage in a public information campaign. Posters and brochures in government offices are merely well-intentioned tokens. Full-fledged advertising campaigns are prohibitively expensive and, some might say inappropriate—at least for an ombudsman's office.

Yet rights which remain too much unknown and thus unused, are hardly worth having and could wither. One answer is found in the initiative of some departmental employees who have made it part of their jobs to inform citizens about the *Privacy Act*. One employee of a local EIC employment centre sent an article which she had written about the Act to the local paper where it was published. An admirable initiative.

Privacy disappointments have been discussed in earlier reports: slippage in the government's good intention to bring Crown corporations under the *Privacy Act* (Air Canada and Petro Canada appear to have escaped completely); delay in bringing forward amendments to the *Privacy Act*; slowness of the private sector to put in place voluntary privacy codes, despite Canada's commitment to the Organization for Economic Co-operation and Development's (OECD) privacy guidelines.

These are mainly grumblings about bureaucratic inertia and missed opportunities. The world does not share a privacy commissioner's sense of urgency. Nothing surprising nor anything inherently damaging about that. What is more likely to send a privacy protector into a blue funk on a bad day is the sheer magnitude of the threat from the new technologies.

Can any data protection regime do more than tinker at the fringes in a world of micro-computers, with their ever larger storage and transmission capabilities, local area networks, machine readable (smart) cards, laser discs, glass fibres, computer-matching, point of sale payments, enhanced databases, machine scanning—to keep the list short? "Is there some point", as Professor James Rule of the State University of New York has asked "beyond which collection of personal data simply becomes excessive, whatever principles may govern the data systems?"

Consider the daunting challenge for data protectors in monitoring a centralized regime of fair information practices in an increasingly decentralized, if not fragmented, environment. A recent OECD paper summarized the functional effects of technological change as "the trivialization of data processing". One could also speak of the "democratization" of access to data-processing through the proliferation, not only of micro computers, but by expert and microform systems, optical discs, two-way cable television.

Four years ago it was reported somewhat breathlessly in one of these reports, that the number of microcomputers in the federal government was about 6,700 units, some 1,700 having been acquired in the previous year alone. Today they are as common as once were manual typewriters. No one seems even to count any more though, for the record, as far as anyone knows, the total appears to be some 30,000.

It is not only that micros have access to larger computers; microcomputers *are* larger computers. Moreover, they possess such extraordinary flexibility that the old concept of what constitutes a file is becoming utterly outmoded. As another OECD report points out, "it is no longer necessary to work with clearly pre-defined file structures; existing file structures can be adapted to new ones".

A file is now more slippery than that "damned, elusive Pimpernel". A file can be opened, blended, collapsed, and reincarnated at a push of a button. A study by the Council of Europe has concluded that some of the old assumptions in data protection no longer apply. The solution envisaged in the 1970s "were valid insofar as they were brought to bear on the then state of the art, characterized by main frame/stand alone computers with dedicated applications capable of storing and processing data on 'identified or identifiable individuals' on a 'file' under the authority of a 'file controller' identifiable at will by a 'supervisory authority'". Now how does a privacy commissioner, as the "supervisory authority", have any assurance that he is seeing a complete file on an "identifiable individual" when a file no longer possesses any definition?

Are dispersed computer files even records? The *Privacy Act*, with serendipitous prescience, was written broadly and speaks of personal information "about an identifiable individual that is recorded in any form". There is no mention of either records or files. The Act is also silent on how much computer programming, if any, must be carried out in a search for personal information.

To their great credit, there is no evidence that Canadian government institutions have circumvented the *Privacy Act* by refusing to give access to personal information if it is not neatly packaged and identified in a single file, either paper or electronic. Yet electronically stored and dispersed information can be instantaneously sorted, retrieved or even destroyed with a few computer keyboard strokes; the temptation to use new technology to thwart the Act grows stronger with each splendid new computer.

How can a privacy commissioner be sure that it is always resisted?

When the processing of data no longer needs to take place within a system of centralized data banks, the effectiveness of existing audit tests for compliance with the *Privacy Act's* rules must also be questioned. New decentralized, interactive and multifunctional computer terminals challenge the capacity of existing auditing methodology.

How can personal information be kept, as it should be, secure and segregated to its original purpose when it is now possible for every computer terminal to be connected, as an OECD paper has noted, through public or private transmission lines, to everybody else's terminal?

The general principles of data protection have stood up remarkably well, precisely because they are general. Every study comes to that conclusion. But the monitoring of technology must be clever enough to match the marvellous abilities of the new generations of computers. Otherwise, data protectors will find themselves merely wringing their hands and filling the air with lamentations. A compelling need in any privacy commissioner's office is to keep up with the technology in order to possess reasonable assurance that their technical experts can challenge the best in the computer business.

"Telecopiers without a technical system guaranteeing data protection must not be allowed to be sold, like a car without brakes."
—Professor Spiros Simitis, Hesse Data Protection Commissioner.

In an ideal world, the developers of new informatics technology are sensitive to the surveillance implications of their products and seek the advice of data protectors at an early planning stage. Alas, it is not an ideal world.

Privacy and the private sector

Pessimistic ruminations on a bleak day should not give way to despair. Those general privacy principles which have stood up so well can be adapted to new technology, to evolving situations. The OECD recently noted that regulatory approaches to privacy protection are moving more generally to "rules governing specific sectors of activity". A sector-oriented approach means tailoring rules to serve the specific needs of, say, banking, telecommunications, direct mailers, the airlines or government.

Rules for one sector can prove to be, unworkable—or ineffective—for another. Flexible codes for meeting challenges to privacy protection are now required for the successful selling of voluntary privacy codes to indifferent, hostile or merely dubious chief executive officers. In Canada, it is still possible to cling to qualified optimism that the Canadian private sector will yet come forward with public commitments to fair information practices. Slow progress continues to be made on a sector-by-sector basis.

In last year's annual report, the Privacy Commissioner stated:

> "Without more evidence of effective self-regulation (in the private sector), however, the supporters of voluntary data protection codes will be increasingly hard put to defend their position".

During 1989-90, the Privacy Commissioner has had extensive consultations with associations representing the air transport, telecommunications and banking industries. While there has not yet been widespread adoption by these institutions of privacy codes of practice conforming to the OECD guidelines, meaningful expressions of intent have been made to move in this direction.

The Canadian Bankers Association's model privacy code, which had fallen into limbo for some years, is back under active consideration for adoption by most of the chartered banks. The Canadian Air Transport Association is working with the International Air Transport Association to adopt a data protection code of practice for customer records and will review the privacy practices in place for employee records. Member companies of Telecom Canada appear willing to organize their already heavily regulated customer records requirements into a privacy code. They are also reviewing their employee records management practices against the OECD privacy guidelines to verify or ensure compliance.

This missionary work showed signs of results at a meeting in Vancouver earlier this year between members of an organization bringing together most of the federally-regulated industries, (FEDCO) and the Privacy Commissioner. There was unanimous support in principle for voluntary codes.

"The global village is very restless."
—Geraldine Kenney-Wallace, President, Science Council of Canada

Time for a nudge

But privacy commissioners have had assurances of action from the private sector in the past; assurances which never became realities. And so, while the actions of these three federally-regulated sectors are positive enough to keep alive the voluntary approach to privacy protection, the law should now give the process a firm nudge.

To that end, the government should consider bringing forth an amendment to the *Privacy Act* requiring federally-regulated firms to develop, implement and submit to the Privacy Commissioner for review, voluntary codes of privacy protection in conformity with the OECD guidelines. It is not necessary for the Privacy Commissioner to have the power to order changes to any such code or to have any role in its enforcement. He should, however, continue to monitor the effectiveness of these voluntary codes and, only if experiences prove unsatisfactory, develop recommendations to Parliament for stronger privacy regulation.

There are also clear trends elsewhere towards self-regulation. Even European countries, which began by compelling the private sector to register personal information holdings with privacy commissioners, are reducing licensing requirements and encouraging self-regulation.

Closer to home, that bastion of free enterprise and holder of vast amounts of personal information, American Express, has now announced to the world that "the issue of privacy will be so important in the years to come that we intend to be an advocate of consumer privacy". An American Express senior executive, speaking on behalf of his company, has said that he was "increasingly concerned by the companies that collect information for one purpose and sell it to another without the individual's consent".

American Express has seen the handwriting on the wall.

The company's own survey of consumer attitude revealed:

- 90 per cent of all Americans do not think companies disclose enough about their list usage practices;

- 80 per cent do not think companies should give out personal information to other companies;

- more than one-third of all Americans think the federal government should regulate the use of lists in their country.

Does anyone believe that Canadian figures would be substantially different? Of course not.

American Express has adopted a voluntary privacy code not out of a sudden intellectual commitment to privacy as an abstract virtue. It became convinced that in 1990 privacy protection has become good business. Good business, first, because, in American Express' words, "companies who respect their customer's patience and privacy will grow stronger in the years ahead; second, because the customer database can become...a tool of destruction that erodes consumer confidence and ultimately takes our future out of our hands and turns it over to the government". This is precisely the message the Privacy Commissioner has been preaching. It should carry more weight in coming now as an unsolicited testimonial from a company with impeccable credentials as a player in the private sector.

Dad: Have you been a good boy so Santa can send you what you asked for?
Son: Oh, I know Santa will send me what I want.
Dad: How do you know that?
Son: Because I'm in Santa's computer.
— Overheard by the New York Times.

During the Year

Public servants' hot line

The year brought the unusual, though surely not unedifying, spectacle of two officers of Parliament giving conflicting advice to their masters.

The issue arose when the Auditor General proposed a "hot line" which would receive anonymous allegations of fraud, waste or mismanagement. He believed that a guarantee of anonymity would encourage individuals to speak, protected as they would be against reprisals, and produce considerable savings to the taxpayer. This cause, of course, is entirely worthy.

The Privacy Commissioner intervened because of his *Privacy Act* responsibility to defend rights. One of those rights is to know what accusations against an individual — and who made them—are recorded in government files. Be they true and well-intentioned, as some may be, or false and malicious, as others may be, it is fundamental to our notion of justice that accusations not be secret nor faceless.

The dispute between the Auditor General and the Privacy Commissioner was a clash of two important values. For this reason, the Privacy Commissioner is grateful to the Public Accounts Committee for its invitation to both the Auditor General and himself to make their cases.

The case of the Privacy Commissioner was that the Auditor General could not, without changes to the *Privacy Act*, offer "whistle-blowers", no matter how public spirited, the guarantee that their identities could be protected. If the Auditor General's office was designated as an investigative body, as set forth under the *Privacy Act*, the names of his informers could be protected. But his office is not in the police business.

The Auditor General suggested in his 1988 report to Parliament that the *Privacy Act* should be amended to make possible precisely what he wanted to accomplish by his hot line.

While a guarantee of anonymity for whistle-blowers may produce savings to the public purse, one wonders what it would do to our public officials—union members and management alike. A Kafkaesque system of justice would be theirs—unknown accusers, unknown allegations, never knowing when or why the inquisition will befall them.

If stronger laws are required to protect whistle-blowers from retaliation, they should be enacted. But a lesson from history (and not so very distant history) is that governments which encourage their citizens to be faceless informers not only exact, but pay, a great price.

It is for Parliament, not the Privacy Commissioner nor the Auditor General, to decide when privacy rights should give way to other values. The Public Accounts Committee has not recommended that privacy rights be pushed aside in this matter. Nor has the Auditor General argued since for his project.

Reviewing the CSIS Act

In November, the Privacy Commissioner made a submission to the Special Committee on the Review of the *Canadian Security Intelligence Service Act*. What follows is largely an extract from that submission.

The major institutions comprising Canada's security-intelligence apparatus, including the Canadian Security Intelligence Service (CSIS), must comply with the *Privacy Act*. Yet Parliament took great care to ensure that the personal information access rights afforded to individuals by the *Privacy Act* would not undermine the ability of government institutions to safeguard national security.

Six years of the Privacy Commissioner's findings and Federal Court decisions, demonstrate the ability of the *CSIS Act* and the *Privacy Act* to coexist, if somewhat warily.

By the nature of its work, CSIS makes difficult judgments about when it is appropriate to target individuals for surveillance. From the privacy perspective, the *CSIS Act* has provided the agency with important guidance which was unavailable to the former RCMP Security Service. Many of CSIS's problems with the *Privacy Act* have been inherited. Most concern information collected by the former security service—whether it was properly collected and whether it can be disclosed without injury to the CSIS mandate.

The solution to this problem is not, in the Privacy Commissioner's view, an amendment to the *CSIS Act*. Rather, it is timely destruction of that information inherited from the RCMP Security Service, the collection of which would now be improper under the *CSIS Act*. That review and destruction process is underway. The Privacy Commissioner is satisfied with the priority CSIS has attached to this task.

In its document, *Amending the CSIS Act*, the Security Intelligence Review Committee (SIRC) recommends:

> "...that Parliament consider the advisability...of adding a paragraph to subsection 39(2) of the *CSIS Act* specifying that the Committee is entitled to have access to any information under the control of the Service, notwithstanding the existence of any investigations that may be undertaken by the Information Commissioner or Privacy Commissioner."

While one may understand SIRC's unease in being denied access to anything it requests of CSIS, section 33 of the *Privacy Act* requires that the Privacy Commissioner's investigations be conducted in private. Moreover, subsection 33(2) provides that "no one is entitled as of right to be present during, to have access to or to comment on representations made to the Commissioner by any other person".

If SIRC's proposed amendment were to be adopted, it would provide it with a right of access to CSIS's representations to the Commissioner and the Commissioner's correspondence to CSIS. This would infringe clearly upon the provisions of section 33.

The limits placed on SIRC's access to CSIS records set out in section 33 of the *Privacy Act* do not, in the Commissioner's view, impede SIRC in the exercise of its mandate. But from the Privacy Commissioner's point of view, those limits are necessary to the proper discharge of his mandate, especially to protect the identities of complainants and to foster candor in the investigation and resolution of complaints. Moreover, Parliament is already assured that one of its own officers has ample power to monitor CSIS's sensitivity to the privacy rights of Canadians.

In its 1988-89 annual report, SIRC said that it had asked CSIS to provide it with the files that had been the subject of a complaint to the Privacy Commissioner and a subsequent application under the *Privacy Act* to the Federal Court of Canada. The reason given by SIRC for this request is:

> "We wanted to assure ourselves that the Service had not unreasonably withheld anything from the Privacy Commissioner's examination".

While the Privacy Commissioner appreciates SIRC's support, this statement reveals a lack of understanding of his role and powers vis-à-vis CSIS.

In conducting investigations of complaints against CSIS, the Privacy Commissioner has extensive powers to enter premises, compel the production of witnesses and documents and take evidence under oath.

Section 68 of the *Privacy Act* makes it a summary conviction offence to obstruct the Privacy Commissioner in the performance of his duties and functions. The Federal Court, too, has a role in ensuring that CSIS respects the *Privacy Act*. The Privacy Commissioner or a complainant may ask the Federal Court to review a decision by CSIS to deny access to requested information.

Surely it carries the notion of "oversight" to an extreme to suggest that SIRC has a role in ensuring that CSIS acts lawfully in its dealings with the Privacy Commissioner and with individuals exercising *Privacy Act* rights. That, in effect, would be reviewing the reviewer, Parliament's reviewer at that. Such a proposal calls into question the effectiveness of the Privacy Commissioner as well as the Federal Court. It even implies misbehaviour on the part of CSIS in its compliance with the *Privacy Act*. Such an implication is unfounded and unfortunate in the light of the commendable effort of CSIS to live by the letter and spirit of the *Privacy Act*.

A parallel monitoring by SIRC of CSIS's dealings with the Privacy Commissioner would send all the wrong signals to CSIS, the Privacy Commissioner, the Federal Court, Parliament and the public.

Consequently, the Privacy Commissioner recommends that any amendment to subsection 39(2) of the *CSIS Act* should not provide SIRC with a right of access to correspondence between CSIS and the Privacy Commissioner related to a *Privacy Act* investigation.

SINning...again

Lest the litany of SIN become a dirge, there were upbeat notes during the year.

Reports on the Commissioner's comments and suggestions about SIN have made the office a lightning rod for much of the public's frustration about trivial uses of the number. Consequently, many calls and letters concern uses well outside his mandate—most of them in the private sector.

Rather than pleading no mandate, the Commissioner has taken to passing on the comments, always emphasizing that their requests are not illegal but often offensive. He uses the opportunity to sell the concept of voluntary codes in the private sector and suggests that a little more sensitivity to SIN requests might reap public relations benefits.

The response has been surprisingly positive from, among others, General Motors, the Canadian Council of Professional Engineers, the University of Western Ontario and J.B. Marketing—a computer technology company.

Some details of these exchanges follow.

An MP had passed on to the Commissioner an advertisement in an engineering journal containing a Mastercard application which required the SIN. The executive director of the Canadian Council of Professional Engineers sympathized with the Commissioner's comments about the growing use of the SIN as "a de facto national identifier".

He replied, "while I concur that requiring the SIN is bad business practice and I will ensure that no further requests for it are made in the Mastercard advertisements...I have to wonder if by now any attempts to guard our privacy come too late." Citing the government's original (1964) commitment to use SIN only for social insurance benefits, he urged the government to "set a good example by not requesting the SIN when processing Canada Savings Bonds purchases."

The Commissioner conceded that the government's admirable new, more restrictive SIN policy had been "muddied" by recent changes to the *Income Tax Act*, but encouraged him not to despair and to continue resisting frivolous requests for the number.

A General Motors newspaper advertisement for a preferred customer card under GM's Smartlease program prompted a call from another MP. This ad also asked for the applicant's SIN. The MP considered the request "an example of excessive use of SIN".

The president of General Motors replied that the Commissioner's letter had given GM an opportunity to test one of its corporate values—to be "customer focused". He wrote: "... all future General Motors advertisements containing a form for customer information will no longer require the applicant's Social Insurance Number".

Two university requests for SIN were also eliminated. One problem was solved by the University of Western Ontario's ombudsman who succeeded in convincing university administrators to stop using the number when issuing locker keys to students.

Another student (at Simon Fraser University) objected to having to produce the SIN to prove that he qualified for a discount when buying computer software. Privacy staff inquired and found the request was contained on an outdated form the company, J.B. Marketing, had provided to the university.

The company told the Commissioner that in revising its American form, the request for SIN had been overlooked. Its education department "attempts to inform our clientele the SIN is not required to process the order". The company suggested the client get in touch with their representative to straighten the matter out.

SIN can be overcome when there is will and consumer resistance.

Thanks to Mr. Statsman

Worthy of special mention in an end-of-term report is the tangible commitment to privacy demonstrated by the Chief Statistician of Canada. It is especially noteworthy because many of the *Privacy Act* requirements do not apply to statistical records. Yet the Chief Statistician has voluntarily established the practice of consulting the Privacy Commissioner on privacy issues concerning statistical records.

Though Statistics Canada data bases are for statistical uses only and cannot lawfully be used in any decision-making process directly affecting individuals, detailed and sensitive profiles of individuals can be compiled from such statistical data. Thus decisions about establishing and linking such information holdings raise privacy concerns.

A project being considered by Statistics Canada will illustrate the point.

Statistics Canada proposes to co-operate on a health survey with the Manitoba Department of Health and the Canadian Institute for Advanced Research. The project would link limited information from the Manitoba health data bank with Statistics Canada data, including some taken from the 1986 census.

This proposal, known as the Manitoba Population Health Pilot Project, would create a statistical data base to help the Manitoba government assess its health care needs and to develop health policy options. Of course, other provinces have expressed an interest and Ontario has lent its strong support.

This proposal is unique because it would link census data with other administrative data bases. While postal codes, and not names or addresses, would provide the link, the resulting data (under the sole control of Statistics Canada) would be information about identifiable individuals. The original data subjects could not have foreseen that the information originally provided to Manitoba and Ottawa would be used to create detailed, sensitive profiles on individual Manitobans.

The Chief Statistician took the initiative, as he has on other privacy matters, and sought the Privacy Commissioner's view on whether the public interest justified conducting this record-linkage.

The Privacy Commissioner agreed that the proposed pilot project had potential for contributing significantly to the public interest; most important, he considered it possible to accomplish the goal without intruding on personal privacy. He suggested protecting the individuals' privacy by stripping away the personal identifiers—in this case the postal code.

Some may consider the *Privacy Act* remiss in not subjecting personal information used for statistical purposes to the same requirements imposed on personal information used for administrative purposes. No one should doubt, however, that the privacy concerns about statistical data are being addressed in practice.

The Chief Statistician of Canada is to be thanked for that.

Spreading the word

An organization's communications function is not usually the subject of an emotional debate. But the role of an ombudsman requires a delicate balance between telling the public he exists without appearing to be generating his own work or damaging his credibility.

Specialist ombudsmen such as the Privacy Commissioner have also to tread the fine line between being an advocate for the principles of their legislation while being seen as impartial enough to mediate disputes. The debate is not new.

The Privacy Commissioner does not have a mandate to tell the public what he can and cannot do as have the Chief Human Rights Commissioner or the Commissioner of Official Languages. However, since his office operates with taxpayers' money and provides a service to "anyone present in Canada", he must try to be visible, accessible and accountable to those who pay the bills.

Although the Commissioner has not allowed the absence of a specific mandate to prevent him from telling Canadians about their privacy rights, the lack of funds restricts this work. After seven years, many legislators and public servants—and, based on anecdotal evidence, most members of the public—know nothing about their privacy rights, a disappointing legacy.

However, strides have been made. During the past year alone, the Commissioner and staff spoke to more than 60 audiences which ran the gamut of government, the private sector, labour and universities. The Commissioner urged the private sector to adopt voluntary privacy codes at meetings of the Canadian Public Relations Society, the Canadian Information Processing Society, the Air Transportation Association of Canada, federally-regulated employers in the transportation and communications sectors and the Issues Management Association.

The Commissioner or his staff have spoken to (among others) a special Statistics Canada seminar considering a proposed match of federal social program data with provincial welfare files; the National Joint Council on employee privacy issues; records managers on the new data matching and Social Insurance Number policies; the Law Hours at Dalhousie University and the University of New Brunswick; and two classes of CSIS recruits.

The office has distributed its information material to members of the Canadian Library Association, L'association des bibliothecaires professionelles du Québec, Employment and Immigration centres in eight provinces and MPs' constituency offices. Public affairs staff have also handled almost 1600 requests for material about the *Privacy Act*, the Commissioner's role and the impact of data protection.

Drug testing: everybody's doing it

Last year's report discussed the threats posed to privacy by new biotechnologies. There was a promise to monitor these developments.

Thus, the Privacy Commissioner's office completed a major study of the impact of drug testing technologies upon privacy and the *Privacy Act*. It is soon to be made public.

The study examines the scientific limitations of urinalysis, the most common drug-testing (other than alcohol) technology. Such testing cannot determine or measure the degree of impairment nor can it verify present use. It can verify only past use, and this with an error rate of from two to five per cent.

For this reason, urinalysis is a tool different from breathalyser or blood tests. The latter can provide confirmation of use and impairment at the time of the test—be that while operating a motor vehicle, or performing some other safety-sensitive function. Urinalysis, on the other hand, can only confirm past drug use—use which may have taken place in the privacy of one's home and have no impact upon the performance of safety-sensitive activities.

The *Charter of Rights and Freedoms* may stand in the way of infringing upon a person's "liberty" to consume intoxicants when it poses no reasonable threat to health or safety. This was the decision of the Quebec Superior Court in the case of *Dion* v. *the Queen* (1986).

Urinalysis testing intrudes into private lives. It is scientifically unsuited to answering the questions of whether an individual engaged in safety-sensitive activities is using, or is under the influence of, performance-altering substances. Yet governments and private sector firms appear eager to use urinalysis to protect the public, find the perfect employee or both.

Transport Canada, for example, is proposing random and mandatory testing of Canadian transportation workers. Privacy concerns notwithstanding, the government is to be commended for initiating a process of public discussion of this proposal, including bringing the matter before Parliament by way of legislation.

There will be opportunities for all concerned parties, including the Privacy Commissioner, to address such hard questions as:

1. Is there reliable evidence of a significant drug abuse problem among transportation workers?

2. Are there available less intrusive means of dealing with such abuses?

3. Are adequate safeguards in place to satisfy a reasonable expectation of privacy? and

4. What role are U.S. testing requirements in the transportation industry playing in determining Canadian testing policy?

These matters are addressed in the Privacy Commissioner's study on drug testing and the *Privacy Act*.

Genetic analysis

Unprecedented research energy is being put into exploring the human gene for the wealth of information it contains about individuals. This area of bio-medical study is opening marvellous new diagnostic avenues, enhancing the possibilities of early detection of disease, improved treatment and ability to avoid the transfer of hereditary conditions. Genetic analysis is also becoming a major tool in the law enforcement field for identifying persons—either to confirm or eliminate suspects.

As with all technologies, however, there is a dark side. Genetic analysis is being explored to determine its reliability as a predictor of future behaviour—pre-disposition to antisocial behaviours or to mental or emotional disorders. The perennial search for the perfect employee is leading some to look to genetic analysis for information on the likelihood that an employee will remain healthy (genetic pre-disposition to cancer or heart disease), be honest and stable and have an aptitude for the job.

In the insurance industry, too, the possibilities of new gene technology have not gone unnoticed. In an industry where AIDS tests are becoming mandatory for life insurance policies over a certain amount—think of the attractiveness of a gene assessment.

Finally, this technology makes possible prenatal selection—with an especially frightening potential for discrimination against those who don't "measure up".

Canadian law has to do some running to catch up to the present state of genetic technology. We are lagging behind other countries and there is much at risk by our slowness.

Germany is on the leading edge. An official commission of inquiry of the German Parliament has already reported on the opportunities and risks of genetic technology. German federal and state privacy protectors have issued guidelines to control the threat gene analysis poses to privacy. Both reports conclude that stringent federal laws are required to control this technology. The recommendations include:

1. limit gene analysis in the criminal justice system to confirmation of identity only;

2. prohibit gene analysis in employment matters;

3. require insurance contracts to state that gene analysis is not a prerequisite and provide assurance that standard consents for disclosure by physicians will not cover genetic analysis information;

4. allow prenatal genetic probing only to reveal a curable condition which would otherwise lead to unacceptable damage to the future health of the child;

5. limit genetic screening of newborns to genetic illness which can be cured or at least substantially controlled by therapeutic means; and

6. require, except in law enforcement, gene analysis only be conducted on the basis of a truly voluntary and fully informed consent.

Such guidelines offer an important groundwork of protection against the dark side of genetic technology. Though some of these recommendations remain open to debate or may be beyond its legislative jurisdiction, Parliament should be aware of the fast-developing issues, do what it can as soon as it can, and prepare legislative proposals to control the uses of genetic analysis.

The Ontario Law Reform Commission and the recently-appointed federal Royal Commission on Reproductive Technology are both examining wider issues in this area and are aware of the possible need to respond to the new genetic technologies.

The Privacy Commissioner will continue to monitor the related privacy issues and keep Parliament informed.

Police databases-CPIC

Some of the most sensitive personal information held by government is in the automated data bases administered by the Canadian Police Information Centre (CPIC).

CPIC's computerized information system has four major data bases to which law enforcement agencies contribute—and from which they can obtain—a wide range of information. According to the RCMP, there were more than 72 million operational transactions on these data bases during the 1987/88 fiscal year; more than 21 million of these concerned individuals.

The centre, federally funded and administered by the RCMP, is governed by an advisory committee of the major municipal and provincial police forces (the RCMP in eight provinces) and the attorneys general of Ontario and Quebec. However, the sole authority for CPIC policy and procedure is the Commissioner of the RCMP.

Since some of the information is contributed by non-federal sources, jurisdiction over personal information in the centre's data bases remains in question. The need for some effective data protection oversight is not.

CPIC was established to provide more efficient handling and exchange of law enforcement information. The RCMP describes the system as "facilitating country-wide access to police information" and "improving the collection, storage and control of records by police forces".

Access to the data bases is controlled according to whether the requestor is a federal, provincial or municipal police force, foreign law enforcement agency or an agency with a limited law enforcement role (such as Canada Customs or Employment and Immigration).

The four data bases are:

1. Investigative Data Bank Files. These include files on missing and wanted individuals (including missing children), stolen vehicles and boats, major unsolved crimes and recovered but unidentified bodies.

2. Identification Data Bank Files. The files include criminal records and the criminal name index.

3. Intelligence Data Bank Files. These files include the Automated Criminal Intelligence Information System (ACIIS) with limited access from 27 terminals controlled by the Canadian criminal intelligence community. There are no foreign interfaces to ACIIS. The information concerns individuals, businesses, vehicles and other subjects. The "Focus" file contains information on organized motorcycle gangs.

4. Ancillary Data Bank Files. These include registered vehicle owners, licensed drivers and information from federal and provincial correctional services.

The RCMP also operates a fifth automated system known as PIRS (Police Information Retrieval System) but not under the CPIC umbrella. PIRS contains information on events, subjects, vehicles and property. The service is operated on cost recovery and is available to other federal departments and to 12 municipal police forces.

After its in-depth review of the *Privacy Act*, the Justice and Solicitor General Committee recommended that CPIC be made subject to the Act and that the Privacy Commissioner audit the data bases to verify that the privacy interests of Canadians were being adequately protected.

The government rejected the recommendation, choosing instead to consult the participating law enforcement agencies on how best to address the privacy issues. After it appeared that no solution was forthcoming, the Privacy Commissioner suggested that the RCMP consult CPIC users to determine whether it could implement voluntary privacy controls over its data bases. These controls would take the form of a comprehensive data protection policy on the collection, use, disclosure and disposal of the information and the creation of access and correction procedures.

The Commissioner made four suggestions.

First, the most difficult aspect of a voluntary code would be to provide an acceptable access and correction procedure. The Commissioner urged the RCMP to go beyond simply referring applicants back to the source agency and to consider making access available to the entire system through a single access point.

Second, he asked that the policy restrict itself to limited, well-defined exemptions, cautioning the force against going beyond the exemptions contained in the Ontario, Quebec and federal privacy legislation.

Third, the Commissioner asked that the policy assure individuals that incorrect or incomplete information will be corrected or deleted in both the automated system and the original records. If there is an unresolved dispute about the accuracy or completeness of any information, it should be flagged as being disputed and a notation of the individual's version included on the file.

Finally, the Commissioner urged the force to provide a mechanism for handling disputes about exemptions, delays and correction requests.

The RCMP responded positively to the Commissioner's suggestions and has already begun applying these principles to its own systems, including the PIRS. The force also presented the Commissioner's views on privacy protection to the CPIC advisory committee which is actively considering voluntary privacy controls.

It is too soon to know whether there is any future for voluntary privacy controls over CPIC. But the police community's willingness to examine the options is reason enough for optimism that a balance can be struck between legitimate law enforcement needs and individual privacy rights.

Ring, ring... Orwell calling

Last year's annual report discussed the privacy implications of a proposal before the Canadian Radio-television and Telecommunications Commission (CRTC) which would require Bell Canada to sell its directory data base in machine-readable form. (At this writing no decision has been given.)

In 1989-90 another telephone privacy issue surfaced.

In this one Bell Canada sought CRTC approval for a number of services, including one which would display the originating phone number of all incoming calls on specially-equipped telephones. This proposal presented a feast of privacy issues. The service would protect subscribers from harassing or simply unwanted calls—a real "plus" for privacy. But it could also render it impossible to make an anonymous telephone call—a privacy "minus".

After some initial hesitation—one is reluctant to prescribe which privacy value is more important—the Commissioner concluded that the privacy minus outweighs the plus. At base, it is unacceptable that we should surrender our anonymity as a necessary condition of using the telephone. The telephone is a basic public service which policymakers cannot treat as optional.

There is public interest, of course, in offering to subscribers a method for deterring abusive or intrusive incoming calls. To choose total loss of anonymity for all subscribers, however, is akin to invoking the *War Measures Act* to deal with a barroom brawl.

Perhaps the issue is not as black and white as it is painted. Is there not some middle ground—some way to give subscribers the proposed technological features while allowing others who can show a legitimate need to remain anonymous to opt out? Other jurisdictions have, for example, given number blocking capability to undercover police officers and to those who help victims of domestic violence. We searched for such a compromise.

In the end, however, the answer is clear: the issue is, indeed, black and white. Ours is not a society where the privacy rights of some are broadly paramount to or imposed upon those of others. The fundamental rights and freedoms contained in our Charter presuppose a carefully guarded underpinning of privacy.

Can one imagine that freedom of expression, of association or belief, or the right to liberty and security of the person, could be meaningful in the absence of strong protections of our privacy? Clearly the answer is "No", and it has already been unequivocally given by the Supreme Court of Canada in such cases as *R v. Dyment* (1989) and *Mario Duarte v. R* (1990).

It would too greatly diminish the state of our personal privacy if every call we made to merchants, government departments, social agencies or media outlets disclosed our identities. To prevent that loss of control surely we are willing to tolerate the fact that some may abuse their ability to call anonymously.

A new exempt bank

This year's news that the Canadian Security Intelligence Service (CSIS) would establish a new exempt bank—with the support of the Privacy Commissioner—demands some explanation.

This is particularly true since the Commissioner has always viewed the concept of exempt banks as contrary to the spirit of the *Privacy Act*, albeit necessary in very limited circumstances.

The tortured history of challenges to the original 20 exempt banks is traced in earlier annual reports. Of the three remaining, Revenue Canada/Taxation's is treated as open and its exempt status will soon be revoked. The RCMP's exempt bank order has recently been revoked and replaced. The new order was necessary because the individual files in the bank had not been reviewed, making the old order invalid. The Canadian Security Establishment's bank was validly constituted and remains closed.

CSIS's proposal to make an exempt bank simply recognizes that SIS/P-PU-010 is already effectively closed. This bank contains information about individuals who are approved CSIS surveillance targets or who have come into contact with targeted individuals or groups. CSIS responds to applications to this bank by neither confirming nor denying the existence of personal information. The *Privacy Act* does not require an agency to confirm that information exists if it "could reasonably be expected" to be exempt under other provisions of the Act.

The philosophy of this approach, simply put, is that it could injure CSIS's ongoing work for persons to know that they were or were not a CSIS target. Both the Privacy Commissioner and the Federal Court (in *Jamshid Zanganeh* v. *Canadian Security Intelligence Service)* have endorsed this position.

Less sensitive intelligence information (for example, about individuals who came to the attention of the former RCMP Security Service) may be released, with appropriate exemptions, from bank SIS/P-PU-015.

The current state of affairs—an officially open but effectively closed bank—misleads the public and may give the *Privacy Act* a bad name. Thus it is better to establish a properly constituted exempt bank.

Such action would put an extra burden of responsibility on the Privacy Commissioner to ensure that an exempt bank contains only information of this most sensitive nature. No exempt bank once established can be allowed to become an uncontrolled hiding place for personal information. Indeed, the *Privacy Act* recognizes this in section 36 by giving the Privacy Commissioner the mandate to examine exempt banks from time to time, recommend that files be moved to open banks, make application to the Federal Court to order the removal if the Service does not accept the recommendation and, of course, to report any non-compliance on the part of CSIS to Parliament.

When CSIS has a functionally exempt bank, as at present, as opposed to an official exempt bank, the Privacy Commissioner is deprived of those oversight powers and, most significantly, the power to apply to Federal Court, under section 43 of the *Privacy Act*, "for a review of any file contained in a personal information bank designated as an exempt bank under section 18". The CSIS proposal to re-establish an exempt bank would correct this anomaly.

However, judging from a statement accompanying the proposal to close the bank, CSIS may be under the impression that closing the bank means it can deny access to the information without having to review the files. That is not how we read the Act. The provision for exempt banks makes it clear that refusing access to an exempt bank is discretionary, not mandatory. Perhaps CSIS will be able to explain to the Commissioner or the courts how it will exercise that discretion without reviewing the file. Responding properly to an application would seem to dictate reviewing the file, regardless of whether the bank is exempt or not.

While CSIS may not have to justify denying access by applying one or more of the nine specific exemptions, anyone who is denied access to an exempt bank can complain to the Privacy Commissioner. Investigators would then review the relevant information and, if it does not qualify for inclusion, CSIS would be asked to remove it and process it as if it were in an open bank.

The Privacy Commissioner would not support granting exempt status to any bank if it would reduce the amount of personal information otherwise accessible to individuals under the Act. However, because of the nature of most of the information now contained in bank 010, and proposed to be included in the new exempt bank, he is satisfied that with or without exempt bank status it will be justifiably kept secret.

Making the bank exempt is the responsible course of action: no more confusion about whether the information is accessible, yet appropriate mechanisms to ensure that the exempt bank is sensitively used.

Complaints Directorate

After successive years of see-sawing complaint statistics—a new counting method in 1986/87, a decrease in 1987/88 and a substantial rebound last year—this report contains no surprises.

The office received 1086 complaints during the year, a modest increase over last year's 1039. Investigators completed 1018, of which 559 were well-founded; 410 were not well-founded and 49 were withdrawn or abandoned.

Fair information code

Another trend continues apace: the steady increase in complaints about breaches of the fair information code contained in sections 4 to 8 of the *Privacy Act*. This code controls the government's collection, use, handling, disposal and security of the personal information it uses to administer its various programs. Since 1984-85 this type of complaint has more than quadrupled.

Canada Post, for example, has experienced a remarkable increase in complaints, particularly those concerning the collection and use of personal information—from 12 in 1988-89 to 61 this year. Clearly, Canada Post employees have come to regard the *Privacy Act* as a mechanism to resolve labour-management disputes. This can be seen as employees challenge demands for more personal information under Canada Post's new leave management policy.

Denial of access

Denial of access remains marginally the largest single category of complaints. Health and Welfare, for example has experienced a large increase in complaints, a number of which concern the issue of ownership and patient access to medical records.

Prior to this year, Health and Welfare denied patients access to even the most routine medical information unless the treating doctor consented. The office succeeded in convincing Health and Welfare to consult only in special cases, a procedure that should reduce the time required to process requests and fewer denials of access.

Time limit complaints

Time limit complaints increased marginally this year. Correctional Service Canada (CSC) remains the number one laggard—responsible for 214 or 50 per cent of all time limit complaints. The Privacy Commissioner considered 78 per cent of these well-founded. National Defence was a distant second with 80, 85 per cent of which were well-founded.

These institutions' time limit problems were first described in the 1984-85 annual report.

While our statistics show a decline in delay complaints across government, CSC has not yet been able to address its problem. Indeed, there is some evidence of an endemic failure by CSC to respect the *Privacy Act's* timeframes.

For example, it became regular practice for CSC to claim extensions for consultation with other government institutions when, so far as the Privacy Commissioner's office could determine, no consultations were undertaken or necessary.

The Act imposes particular difficulties for CSC and at the highest level respect for the spirit and letter of the law has often been demonstrated. However, there has been ample time in seven years under the Act for CSC to allocate adequate resources and establish efficient administrative procedures. Federal inmates make significant use of the *Privacy Act* to obtain their records and CSC is aware that Parliament gave offenders the same rights under the Act as it gave other individuals.

It seems that the CSC bureaucracy simply feels that inmate privacy rights are at the bottom of its priorities.

CSC has eliminated the excessive delays of seven and eight months that once plagued applicants as requests now get responses in 70 to 80 days.

This improvement does not put CSC in compliance with the 30-day response time specified by the *Privacy Act*. That would require substantial procedural changes.

National Defence (DND) appears to be on the way to solving its problem. DND continues to receive almost half of all applications made under the *Privacy Act*, many as a result of its policy requiring members to apply formally under the Act to see their personal evaluation reports. To its great credit (abandoning a long-defended policy takes some doing), DND has decided to treat informally requests for the current evaluation. Not only will this lead to a decline in complaints to the Privacy Commissioner—it could also reduce significantly the number of formal applications to DND.

The lower numbers mean a loss only of a bureaucratic process. This informal approach keeps with the spirit of the *Privacy Act* and marks the end of years of nagging by the Privacy Commissioner and, even, Members of Parliament.

Grounds of Complaints and Investigation Results

Grounds	Discontinued	Well-founded	Well-found. Res.	Not Well-founded	Total
Access	11	36	137	259	443
Use & Disclosure	11	14	19	28	72
Correction/Notation	—	—	5	21	26
Time Limits	27	317	10	68	422
Language	—	—	1	2	3
Index	—	—	—	1	1
Collection	—	13	3	13	29
Retention/Disposal	—	4	—	18	22
TOTAL	**49**	**384**	**175**	**410**	**1018**

New Activities

The directorate embarked on two new activities during the year: assessing proposed new data matches and reviewing section 8(2)(m) notifications. For more detail on these notifications see **Notifying the Commissioner**.

Data Matching Review

The government's data matching policy took effect at the beginning of this reporting year. The policy requires government agencies to notify the Privacy Commissioner's office 60 days in advance of any proposed new data matches of personal information. This permits the Commissioner to act as an advocate for those who may be affected by the match.

The 60-day period allows the Commissioner's office to judge the proposed match against such criteria as:

*assessing the advantages of the match against other approaches;
*verifying that the proposed match relates directly to an operating program or activity of the institution;
*considering whether the information could be collected directly from individuals and if not, why not;
*determining whether individuals should be notified of the new use and if not, why not;
*ensuring that the new data will be as accurate, up-to-date and complete as possible;
*determining the time-frame of the proposal, and
*determining whether individual consent is needed to match the data;
*analyzing the costs and benefits of the matching operation.

Following the assessment, the Commissioner can make recommendations about the matching proposal to the head of the institution. The decision to match or not is, ultimately, made by the responsible minister, not the Privacy Commissioner. Of course, the Commissioner may report any serious concerns directly to Parliament.

The privacy staff examined one such match—a new Treasury Board system designed to coordinate departments' responses to access to information requests. The new system aroused fears among users of the *Access to Information Act* that it would reduce the amount of information available (because it would curb some departments tendency to respond more generously than others).

CAIR system

The new system is called CAIR and is not, technically speaking, a data match. It is a network of microcomputers which provides access to a central database of information about departmental access to information requests. Under the plan, departments are required to provide details of access requests to CAIR, which serves as a central reference and communication system for government access policy. Thirty-two departments are linked to the system.

The office examined CAIR to determine whether personal information about applicants could be retrieved from the database. The answer was an unqualified "no" as personal information is not entered into the database and, therefore, no breach of confidentiality is possible. As well, applications are described in a way which would make it unlikely that identities could even be inferred from the text. The investigator also found the system to contain comprehensive and effective security measures. The conclusion was that CAIR does not jeopardize access to information applicants' confidentiality.

The office is also examining three existing Employment and Immigration Canada (EIC) matches to follow up the office's assessment of EIC's internal privacy audit (1988-89 annual report). The matches include comparing Canada Job Strategy files with Unemployment Insurance (UI) Benefit files, immigration files with Secretary of State files and UI Benefit files with British Columbia Social Services files. The evaluation continues.

A third matching assessment is in its infancy and results from the new Good and Services Tax (GST) which will require some matching programs. For example, Revenue Canada anticipates matching GST and Income Tax data. The legislation also requires individuals and sole proprietors to register with their Social Insurance Number. Revenue Canada considers the SIN "the most effective means of cross referencing". The Privacy Commissioner's office is waiting for a detailed submission on the proposal.

The office has also been approached informally by External Affairs to examine a new single personnel data base to replace several stand-alone systems now in use. The Commissioner is waiting for more detail.

Debts deducted from subsidy cheques

A journalist wondered whether the federal government was breaching the *Privacy Act* by deducting outstanding debts from farmers' drought subsidy cheques.

According to the journalist, Agriculture Canada had withheld from the cheques any money owed on farm improvement loans guaranteed by the federal government, debts from cash advance or special grains programs, money owed to Revenue Canada or in default of support payments to spouses. The journalist asked whether Agriculture Canada had conducted a data match to determine what was owed and, if so, did it comply with the Act?

Agriculture Canada told the investigator that as farmers applied for drought assistance, they were to "understand and agree with the terms and conditions contained in the guidelines to the application form and further agree to any adjustment or refund to the Government of Canada that may be required". The conditions included a consent to release information about their farm operations to "any other government department, agency or corporation" and to various provincial agencies and marketing boards.

Clearly, farmers had been told of the conditions and had consented to them and to any releases. The investigator also found that there had been no data match with Revenue Canada files, although one individual's refund had been reduced at Revenue Canada's request. The application form did provide for offsetting refunds against defaulted family support payments, but this program is not yet operating.

The Commissioner concluded that there was no need for a formal investigation but reminded Agriculture Canada to advise his office of any considered data matches.

Notifying the Commissioner

In general, the *Privacy Act* prohibits federal government agencies from releasing personal information to anyone other than the person it concerns. As with most rules, there are exceptions. The act has 13—from releases to comply with a warrant or subpoena, to information to help validate aboriginal peoples' claims or grievances. Two such exceptions require the government agency to notify the Privacy Commissioner. The first covers releasing information "in the public interest" or to benefit the person concerned. Notification gives the Commissioner an opportunity to advise the person should he consider that necessary.

The second exception deals with releases for a use which is consistent with the purpose for which the information was collected but which has not been described publicly in the *Personal Information Index*. New consistent uses must then be included in the next edition of the Index.

There is some confusion about the Privacy Commissioner's role in examining proposed releases "in the public interest". Yet, the Act is clear.

The decision that personal details are of public interest rests with the head of the government institution, usually the minister, not with the Privacy Commissioner. The Commissioner is notified so that, if he believes it appropriate, he can inform the person whose information is being released. (The drafters of the law might also have anticipated that departments would be more circumspect in claiming "public interest" if they had to notify an independent ombudsman.)

The Commissioner cannot prevent the release or require that particular details be withheld—nor can the person concerned. This helplessness is an anomaly, particularly when compared with third parties' rights to block releases under the *Access to Information Act* all the way to the Supreme Court. The Privacy Commissioner has argued before that individuals too should be able to prevent unwarranted or damaging release of their information before it happens.

In practice, privacy office staff has always been ready to discuss a proposed release, which sometimes lead to a department rethinking its approach. The Commissioner remains apart from these conversations to preserve his independence to investigate any complaints that the release was improper.

The following examples are selected from the 32 notifications received during the year.

Doctor's evaluation reports

National Defence informed the Privacy Commissioner that it intended to disclose evaluation reports about a military doctor to a provincial college of physicians and surgeons.

The Forces had audited the doctor's medical unit and his personal competence and then released him from service. Because of the release and the doctor's standard of medical practice, the provincial college asked for the audit reports to help in its own evaluation of the doctor's competence as a physician. The college was concerned that the general public should be assured that licensed doctors meet a minimum acceptable level of medical competence.

The Commissioner notified the doctor of the release.

Japanese Canadians' records released

The Japanese Canadian Redress Secretariat asked National Archives for material in its files from the Vancouver office of the Custodian of Enemy Property.

The information concerns Japanese Canadians who were interned during World War II. It includes the minutes of advisory committees on disposal of property, correspondence, ledgers containing entries on money held in trust and real estate, and business records.

The secretariat considered (and Archives agreed) that the release would be in the public interest as it would allow the government to compensate an anticipated 12,000 Japanese Canadians eligible to benefit from the program.

The Commissioner saw no reason to object.

Reports on two inmate escapes

Twice during the year, Correctional Service Canada (CSC) told the Commissioner that it intended to make public detailed reports on escapes by federal inmates.

The independently-prepared reports described the circumstances surrounding the escapes of two convicted murderers, including names and some personal details about both federal employees and private citizens.

The first report concerned Allan Légère's escape while he was being treated at the Georges Dumont Hospital in Moncton, New Brunswick. Légère was considered dangerous and was suspected in a number of murders while at large. The local population was very concerned. He has since been recaptured.

The second report described the circumstances surrounding the escape of Daniel Gingras while on an escorted day pass from the Edmonton Institution. Gingras had overpowered his guard and stolen the car in which they were riding. He was later convicted of two murders committed while he was at large.

In both cases, CSC believed that there was a substantial interest in the public understanding what had led to the escapes and in being reassured that any mistakes in procedure had been corrected.

The Commissioner wrote to all the parties named in the reports, other than the escapees, to tell them of the circumstances of the release.

Woman seeks citizenship confirmation

Secretary of State told the Commissioner it intended to confirm the Canadian citizenship of a man for his sister-in-law. The man, whose wife had died, had left the country and apparently abandoned his two daughters. The provincial youth authority needed the information in order to rule on the aunt's application for custody of her two nieces.

The Commissioner agreed.

Immigrant's details released

Employment and Immigration (EIC) advised the Commissioner that it intended to brief an MP who was pressing the government to have a man removed from Canada.

The MP believed the man's membership in a particular organization precluded his being considered for permanent residence. EIC proposed to release a number of details to convince the MP that the man qualified for entry.

While the office was examining the proposal, a journalist asked the Commissioner whether he had approved the release. Apparently the MP had already been briefed.

The Commissioner told EIC that he doubted that the release was appropriate. He told the man the details which the MP had been given and advised him of his right to complain.

Ex-employees' privacy

Federal employees don't lose their privacy when they retire. This was illustrated when Supply and Services Canada (DSS) called the office about a request for a list of retired government communications officers.

Emergency Preparedness Canada wanted the list to reach former staff to determine whether they were prepared to be on standby during a major emergency. Emergency Preparedness asked DSS to provide the names and addresses.

DSS staff, uneasy about the request, called our office to discuss the proposal. DSS had rejected the request but wondered whether doing the direct mailing was a proper use of the lists which are assembled to mail pension cheques.

After the discussion, DSS denied the Emergency Preparedness request. It suggested getting in touch with communications people before they retire.

Some Cases

Supervisor's diary a departmental record

A Toronto-area man complained that Public Works Canada (DPW) had denied his request to see a notebook about him that his supervisor was keeping. Communications had broken down between the two men and the supervisor was keeping a diary to document the complainant's work behaviour.

The complainant alleged that the diary was kept in the supervisor's locked filing cabinet. When DPW reviewed the diary it exempted its entire contents, claiming that it concerned another individual (the supervisor) and that its release could endanger him.

When DPW learned about the complaint, it argued that the diary should not have been reviewed at all since it was the supervisor's own personal property and not "under the control of the government institution". DPW also challenged the Privacy Commissioner's jurisdiction to investigate a complaint about "private property".

When privacy staff asked to examine the diary it became apparent that the department could ask the supervisor to produce the diary at any time (for example, in response to the original privacy application) and, therefore, it was under DPW control.

The investigation also revealed that the supervisor had begun keeping the diary after a discussion with a more senior manager. All the entries dealt with the complainant's comings and goings and activities on the worksite. The supervisor had prepared the notes in his capacity as a public servant and the information could be used for such work-related purposes as preparing evaluations or responding to grievances. Therefore, it was subject to the *Privacy Act*.

The diary contained little information about anyone else and did not qualify as the personal information of the supervisor. This discovery called into question DPW's original exemption on the ground that the information concerned other staff members. DPW had also maintained that the supervisor had begun the diary because he believed his safety was being threatened and he might need a record in the event of legal action. However, the supervisor told the investigator he did not believe releasing the diary would threaten his safety. Despite a series of meetings, the department and Commissioner's office continued to disagree on control of the diary. Staff continued to try to resolve the impasse and, following several months' discussions, DPW agreed to give the complainant a photocopy of the diary pages after removing information about other individuals.

The Commissioner considered the complaint well-founded.

...But not board members' aides-memoire

A somewhat similar case reveals some fine distinctions between information intended to be used for an administrative purpose (as in the DPW case)—and notes taken as an "aide memoire" by a member of a quasi-judicial board.

In this case a former government employee was denied access to notes taken by an adjudicator during a hearing of the Public Service Staff Relations Board. The adjudicator was hearing the man's appeal of his discharge for unauthorized use of the government telephone system.

Adjudicators take copious notes during the hearings because the proceedings are not taped and no transcript is prepared. Their notes must reflect all the evidence presented and issues raised, not simply the conclusions reached. They then write their decisions using their notes as a reference. These notes are usually destroyed once the decision is released. In this case they were not.

When told of the complaint, the board argued that the notes were the personal property of the adjudicator and not controlled by the board, even though they were in his office. The board cited jurisprudence which supports that position. However, without prejudicing the argument, the adjudicator agreed to let the privacy investigator examine the 92 pages of notes.

There was no doubt that the information concerned the applicant but it was all essentially a recording of the evidence presented in an open hearing. The notes themselves were not evidence and were not used for an administrative purpose. The Commissioner concluded that the notes were not under the board's control and therefore not subject to the Act.

The Commissioner also observed that, even if the notes were under the board's control, they could be withheld under another section of the *Privacy Act* which allows exemptions of information which could harm the administration of a law. He considered that examining an adjudicator's notes could harm administration of this and similar acts by attempting to get behind the decision. The Commissioner concluded that the complaint was not well-founded.

Costs to be borne by department

One complaint prompted the Commissioner to remind Health and Welfare Canada (HWC) that costs to provide access must be borne by the department. The complaint concerned HWC's response to a Nova Scotia man's request to see the file which contained his application for a Canada Pension Plan disability which had been denied.

The man complained that he had waited two months for "useless" information—in excess of the 30 days allowed. The complainant told the investigator that one of two doctors' reports about him had been withheld because seeing it would not be in his "best interest". Although the doctor had refused to release the report, he had agreed to discuss it with his patient. According to HWC, the man would have to pay any charges for the consultation.

A fairly straightforward complaint became a headache when HWC failed to respond to the complaint notification or to return phone calls. The problems were compounded when the investigator went to examine the material and discovered that the entire file had been lost—the disability application, the appeal of the HWC decision and the record of his privacy application.

Medical information can only be withheld from the patient when the department can demonstrate that the release would be contrary to the individual's best interests. HWC staff conceded this would be difficult to prove since the file was lost. HWC also agreed that it was improper to charge applicants for any procedures under the *Privacy Act*.

The complainant consulted the doctor as suggested and was not billed. He does believe that the doctor charged the provincial health care plan for the consultation.

The file remains lost. However, HWC has introduced new logging and handling procedures for all personal files and has begun a pilot project on a new tracking system.

The Commissioner concluded that the delay complaint was not well-founded since departments may take up to 30 days longer to consult other parties (in this case the two doctors). HWC claimed to have mailed the information 56 days after receiving the request and so met the 60-day deadline. However, the complaint that access was denied was well-founded since the Commissioner could not examine the information to determine that it had been properly exempted. The complaint that the applicant was to be responsible for any charges was also well-founded.

40-year old mistake corrected

An Ontario man wrote to the Commissioner in a last ditch effort to have National Defence pay what he alleged was a 40-year-old debt.

The man had served in the British forces during World War II and was entitled to an end-of-service gratuity. When the British notified the man in September 1946 that the gratuity would be paid in Canada, he wrote back to ask how it had been calculated. The British Admiralty responded in November, referring to "the payment made to you recently".

In the meantime, he had received his Canadian gratuity but not the British payment which should have been included. When he asked National Defence for the money, it refused, apparently relying on the British letter as proof that he had already been paid.

The man pursued the matter over many years, enlisting the help of a number of MPs and defence ministers. Each time his request was denied because DND relied on its latest correspondence to prove that he was wrong. Yet, no-one checked the original documents to see where the mistake had been made.

As a last resort, the complainant applied under the *Privacy Act* hoping to bypass all the subsequent letters and to examine the original documents in his pay account. He complained to the Commissioner when none of the material he received established that the payment had been made. He alleged that material he needed must have been withheld.

The investigation unearthed nothing new—he had received everything in the file. It appeared from an old pay document that the British payment was credited to the man's account. The disputed amount was then noted as being paid on the basis of the Admiralty letter. It was then deducted from the total owing.

The Commissioner concluded that DND had not denied access to any material. There was no documentary proof that the payment had been made. The Commissioner wrote to the complainant with his finding, suggesting that he show the Defence Minister the letter because it might help resolve the 40-year dispute.

When the office followed up, the man had moved and left no forwarding address.

Returned mail identifies inmate

An inmate complained to the Commissioner that Kingston penitentiary staff had returned two of his parcels, advising the senders that as a federal inmate he was not permitted to receive them. He considered that disclosing that he was an inmate was an unwarranted breach of his privacy.

The two packages, one from the U.S. Senate and the other from the Manitoba tourism department, contained road maps and travel material. Inmates are not permitted road maps and brochures describing the area around the penitentiary because they could be used to help an escape. The man had been allowed other travel material.

Correctional Service Canada (CSC) told the investigator that inmates may not receive "radios, books..etc.". All parcels are opened and searched for contraband then, if they are unauthorized, are re-sealed and returned to sender with a note quoting the relevant section of the penitentiary's standing orders. CSC maintained that the fact that someone is in a federal penitentiary is public information.

The Commissioner pointed out that CSC's own disclosure code does not permit releasing the inmate's location. Doing so is considered counterproductive to the inmate's eventual reintegration into society.

In the meantime, the inmate had lodged an internal grievance on a number of issues, including this one. When the grievance was upheld at the second level, Kingston penitentiary stopped identifying addressees of returned parcels as inmates.

The Commissioner recommended that CSC establish a policy to ensure that this disclosure not be repeated. Early this year, CSC issued a policy to all its regions requiring mail to be returned "with sensitivity".

According to the new policy, "simply marking the unauthorized package or mail as 'refused' and returning to the return address, with no further explanation, is sufficient...".

The Commissioner considered the complaint well-founded and resolved.

Complainant sees board documents

A man complained to the Commissioner when Canada Post denied him access to submissions to a review board and its final report.

He wanted to see all material examined by the board to determine whether Canada Post had had sufficient evidence of his distributing hate propaganda to warrant intercepting his mail.

Canada Post restored his mail service after the board's public hearing and report.

The complainant also alleged that Canada Post had given the report denied to him to a third party who quoted from it during a newspaper interview.

Initially, the privacy investigator found that Canada Post had not reviewed the material page-by-page, deciding that withholding the entire ten-volume file could be substantiated under a variety of exemptions. As a result of the investigator's request, staff reviewed the file and claimed the following specific exemptions.

*information provided in confidence by another government (section 19);

*information obtained or prepared by an investigative body (section 22(1)(a));

*information which could threaten the safety of individuals (section 25);

*information about other individuals (section 26);

*information subject to solicitor-client privilege (section 27).

Canada Post's Security and Investigations Services is an investigative body under the *Privacy Act*. Thus, most of the requested information could be withheld. However, the board report did not fit this exemption category, nor did documents submitted to the board hearings by the Canadian Civil Liberties Association (CCLA) and an expert witness.

Canada Post agreed to reconsider this material and withdrew its claim that releasing some of the material would endanger other individuals.

Following months of negotiations, Canada Post allowed the man to examine the board's report and the expert witness's submission. When the CCLA submissions continued to be withheld, the privacy investigator suggested Canada Post seek CCLA's permission to release. The CCLA agreed and Canada Post made the documents available.

The Commissioner concluded that the other exemptions were valid and considered the complaint well-founded and resolved.

The office could not investigate the man's allegation that the report had been improperly disclosed because it happened before the *Privacy Act* came into force.

Police told inmate to see reports

Information supplied by other governments "in confidence" must be withheld under the *Privacy Act*. The outcome of investigations into denied release is often a foregone conclusion: If a provincial or municipal government designates the informa ion confidential, it may not be seen

In two cases, however, the privacy investigator found that both National Parole Board (NPB) and Correctional Service Canada (CSC) withheld the same information from an inmate even though the parole officer told the city police force that the inmate would see the information it provided and the force had agreed.

The investigator found other information received in confidence from the provincial government had been similarly exempted. The Commissioner concluded that the provincial government information had been properly exempted but not so the police force material. Both NPB and CSC agreed to release.

Income tax data in harassment file

The *Privacy Act* specifies that information gathered for one purpose may not be used for another unless the secondary use is consistent with the original purpose.

Thus, a Revenue Canada, Taxation employee complained that the department had used his income tax information in a harassment investigation.

At the same time as the complainant was being investigated for the disciplinary matter, he grieved that he had been wrongfully selected for a tax audit. The privacy investigator examined the harassment investigation file and found several references to the complainant's tax situation. He also found evidence that the harassment investigator had access to the complainant's income tax return.

The Privacy Commissioner considered that the tax information should not have been in the harassment file nor should the harassment investigator have had access to the income tax return.

When the Commissioner told Revenue Canada that the complaint was well-founded, the department asked him to consider new facts. The Commissioner agreed, but further interviews uncovered nothing new. Though there was income tax information in the man's personnel documents, Taxation management insisted that it had disciplined him because of the outcome of the harassment investigation and not because of tax information.

The Commissioner could not say conclusively that the tax information had been used for discipline purposes, but the "mere presence of such information in unrelated files constituted a misuse...under the *Privacy Act*". He reiterated that the complaint was well-founded.

No details from other employer

A Nova Scotia man challenged Canada Post's collection and disclosure of his personal information to process his claim for worker's compensation. He had gone to work for Canada Post during a postal strike while on leave from another job. He was injured on his first shift and claimed compensation.

Employers documenting a worker's compensation claim must describe the tasks the employee would be expected to perform on return to work and provide a medical assessment of the employee's fitness to perform those tasks. Since the man was not a full-time Canada Post employee, the corporation obtained the information from his other employer and a Canada Post-appointed doctor. It then sent the information to the Nova Scotia Worker's Compensation Board for adjudication of the claim.

The privacy investigation had to determine whether Canada Post's collection and disclosure of this information was required by the *Workers Compensation Act*. To do so, the Commissioner asked the board to describe what information employers are required to provide to support such a claim.

From the board's response the Commissioner concluded that Canada Post had authority to collect information about the circumstances of the injury at its worksite but it was neither authorized nor required to collect information from the other employer. Further, the board did not ask Canada Post for details of the complainant's medical fitness to return to work. Apparently, the complainant was never told who would receive the medical report.

The Commissioner concluded that the complaint was well-founded. Canada Post has since drafted new procedures to govern compensation claims for anyone injured on Canada Post premises but who is substantively employed elsewhere.

Can't use compensation claim to fire employee

A Correctional Service Canada (CSC) employee told the Commissioner that CSC had ordered her to undergo psychological testing to support her claim for workers compensation, then used the medical reports to fire her.

The woman, a case management officer in a federal penitentiary, was ordered to take the tests to support her claim for compensation for stress brought on by sexual harassment by inmates.

The investigation confirmed that the tests had been conducted to document her compensation claim and that she had not been told the results would be a basis for dismissal. In fact, CSC also used the results to reject her application for another job.

The Commissioner concluded that CSC had misused the test results and that her complaint was well-founded. He asked CSC to guarantee no such situation would recur. CSC has since distributed an employee privacy code to its staff.

Medical details need not be given

Several employees of Canada Post's (CPC) Huron region complained that the corporation was threatening to discipline anyone who refused to complete "voluntarily" a consent for their doctor to give medical information to Canada Post.

The investigation revealed that in each case the employee had taken sick leave and completed the required occupational assessment form on their return to work. Local CPC management was dissatisfied with the form (which does not include a diagnosis) and asked employees to consent to their doctors giving Canada Post medical details.

Employees who refused to sign the consent form were disciplined for "insubordination" and warned that continued refusal would lead to dismissal.

Canada Post headquarters, when told about the complaints, ordered the practice immediately stopped and the regional director of labour relations rescinded dismissals brought to his attention. However, despite the promised resolution, the complaints continued. There seemed to have been a breakdown in communication.

Finally, Canada Post HQ instructed all its divisional general managers that they had no right to detailed, medically- sensitive information and that signing a consent to release this type of information must be strictly voluntary. Canada Post agreed to rescind any disciplinary actions and to pay employees for any days suspension they had served.

Partners' information common to all

Several complaints against Revenue Canada, Taxation required the office to examine difficult legal issues concerning the access rights of limited partnership members to tax information common to all members.

Members of a partnership wanted to appeal their individual tax assessments after Revenue Canada disallowed losses and investment tax credits claimed by the partnership in 1985. Thus, they applied to see information that included details of negotiations between the general (or managing) partner and Taxation.

Taxation claimed that releasing the information would injure the administration of the *Income Tax Act*. The department also invoked the tough confidentiality clauses in section 241 of that act which prevents release of tax information to anyone other than the individual taxpayer it concerns. These provisions, which make Taxation officials criminally liable for breaches of confidentiality, were considered to supersede the access right in the *Privacy Act*.

The applicants in this case received more information after the *Income Tax Act* was amended in 1988 to clarify what material an individual could receive to appeal a tax decision. However, the new release did not deal with information denied under the *Privacy Act*.

The partnership in question was established under the *Manitoba Partnership Act* which specifies that members may "inspect the books of the firm and examine... the state and progress of the partnership business". As well, members of a limited partnership have an individual relationship with Taxation and partners are individually responsible for paying their taxes. The information the members sought was personal about each of them but it was also common to all.

Taxation claimed that since the information concerned each member, it could not release it to any other member without the consent of all the others. The Commissioner maintained that since the information was personal and concerned each complainant, Taxation could not exempt it just because it was identical to information about all the other partners. He held that doing so would effectively deny each individual's right of access under the *Privacy Act*. He also asked Taxation to demonstrate the injury caused the *Income Tax Act* by providing access.

The Commissioner did agree with a number of exemptions which denied personal information that concerned only particular individuals, information supplied in confidence by a province and information exchanged by Taxation and its lawyers which is protected by solicitor-client privilege.

Following weeks of discussions, the department agreed that it could not demonstrate any injury to the *Income Tax Act*. It also agreed that the personal information which was common to each partner should be available to all.

As a result more than 2,000 pages of material were released.

Origin of Completed Complaints by Province and Territory

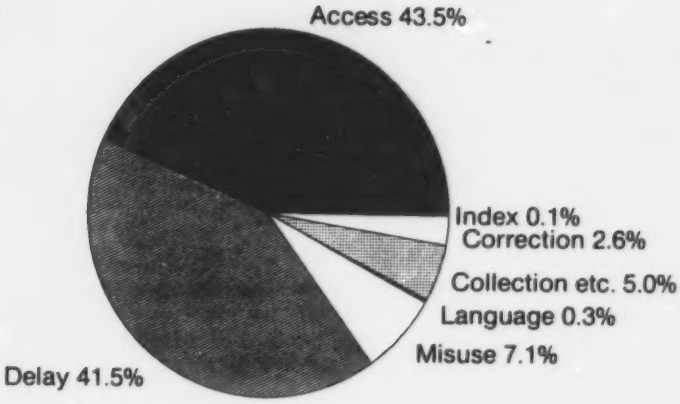
Newfoundland	6
Prince Edward Island	7
Nova Scotia	57
New Brunswick	39
Quebec	147
National Capital Region Quebec	1
National Capital Region Ontario	102
Ontario	362
Manitoba	58
Saskatchewan	39
Alberta	80
British Columbia	113
Northwest Territories	2
Yukon	0
Outside Canada	2
TOTAL	1018

Completed complaints by department and result

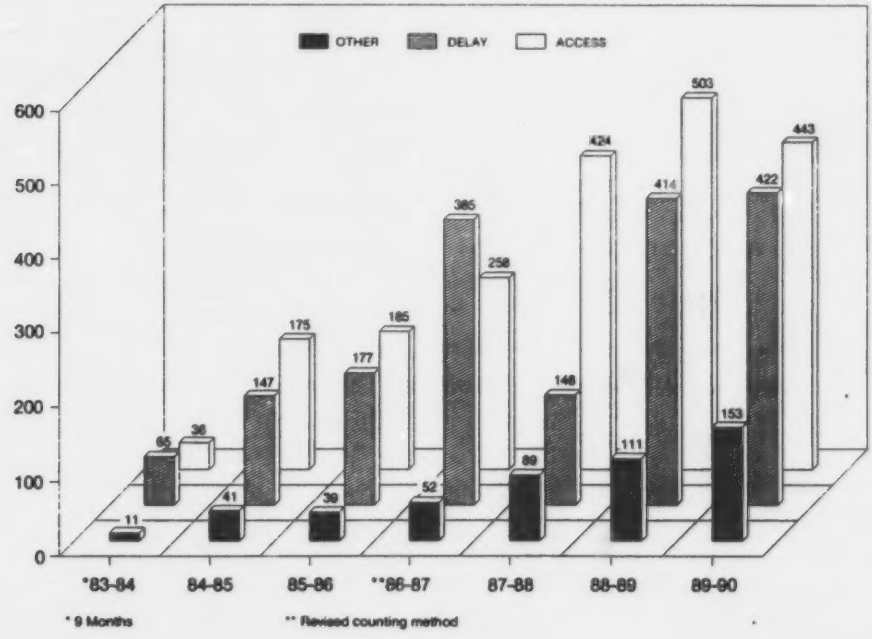
Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Discontinued
Agriculture Canada	1	0	0	1	0
Canada Mortgage and Housing Corporation	1	0	1	0	0
Canada Post Corporation	61	21	9	30	1
Canadian Aviation Safety Board	1	0	1	0	0
Canadian Human Rights Commission	1	0	0	1	0
Canadian Radio-television and Telecommunications Commission	43	1	0	42	0
Canadian Security Intelligence Service	38	2	4	32	0
Commissioner of Official Languages	5	0	2	1	2
Communications, Department of	3	0	2	1	0
Correctional Investigator	1	1	0	0	0
Correctional Service Canada	395	188	59	122	26
Employment and Immigration Canada	53	13	18	17	5
External Affairs Canada	5	1	0	4	0
Farm Credit Corporation	1	0	1	0	0
Health and Welfare Canada	67	25	16	23	3
Indian and Northern Affairs Canada	10	0	0	10	0
Justice	7	1	3	3	0
Labour Canada	5	0	1	3	1
Medical Research Council of Canada	1	0	0	1	0

Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
National Archives of Canada	8	0	1	7	0
National Capital Commission	1	1	0	0	0
National Defence	117	74	14	25	4
National Parole Board	29	5	13	11	0
Privy Council Office	1	0	0	1	0
Public Service Commission	15	1	4	9	1
Public Service Staff Relations Board	1	0	0	1	0
Public Works Canada	3	1	2	0	0
Revenue Canada - Customs and Excise	7	2	3	2	0
Revenue Canada - Taxation	59	38	11	7	3
Royal Canadian Mint	1	1	0	0	0
Royal Canadian Mounted Police	47	4	6	35	2
Secretary of State	2	0	0	2	0
Solicitor General Canada	15	0	1	14	0
Supply & Services Canada	1	0	0	1	0
Transport Canada	7	4	2	0	1
Veterans' Affairs Canada	5	0	1	4	0
TOTAL	**1018**	**384**	**175**	**410**	**49**

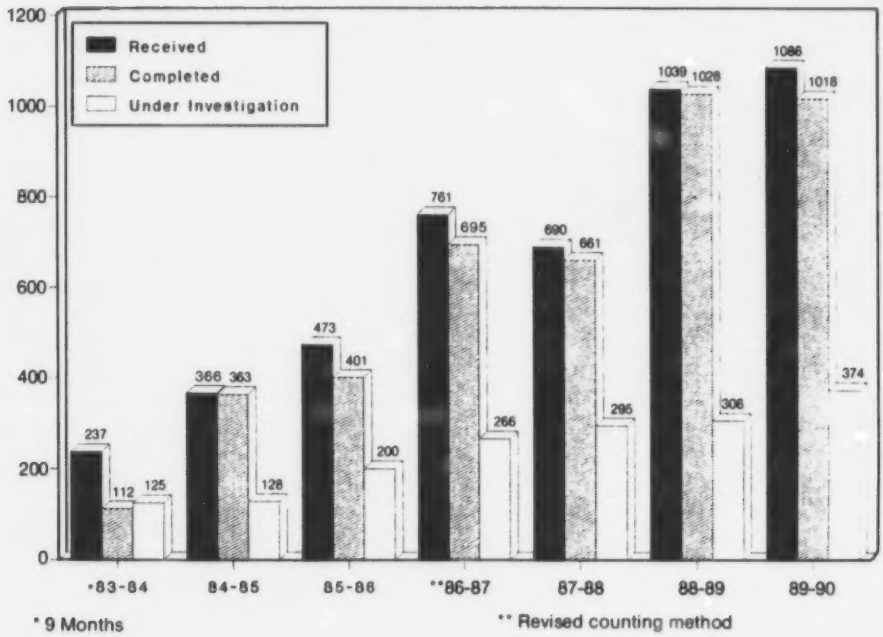
Complaints Completed By Grounds 1989-90



Completed Complaints and Grounds 1983-90



Completed Complaints 1983-90



* 9 Months

** Revised counting method

Inquiries

Once again, the number of inquiries to the office took a substantial leap: 3447 compared to 2041 the previous year. The increase reflects real growth in workload (rather than just better recording which accounted for some of last year's increase). This growth will require the office to hire another staffer next year to help field the calls and letters.

A larger share of this year's inquiries dealt with understanding the *Privacy Act*—59 per cent compared with 46 per cent the previous year. Callers were concerned about employers' requests for medical information or identification documents such as marriage or birth certificates. In one instance, a caller had been asked for a complete list of his personal expenditures. Calls of this type sometimes evolve into complaints.

Public service union representatives were frequent callers on a variety of issues. One asked whether the union could demand a list of its members' actual salaries (rather than salary ranges which are public under the Act). The member wanted to confirm that the employer was remitting the correct dues. Staff suggested the union hire an independent auditor to confirm the accuracy of the information rather than seeking its release.

MP's called and wrote to refer their constituents' privacy concerns. One constituent was concerned about telephone surveys by Statistics Canada. The writer objected to answering personal questions over the telephone since he could not confirm the caller's identity. Statistics Canada is using the telephone increasingly to conduct surveys. However, it usually notifies in advance by letter or telephone those being surveyed and supplies a number for the person to call to confirm that the interviewer is genuine.

Calls about Social Insurance Numbers (SIN) dropped marginally to 19 per cent from 21 per cent a year earlier. Many callers continue to be concerned about the new reporting requirements in the amended *Income Tax Act*. One woman who had been exempted from using the number for religious reasons asked for the office's help because the amendments mean that she could be penalized by law for refusing to supply the number. Staff discovered that, contrary to American practice, no Canadian can be exempt from having a SIN, even on religious grounds.

Queries about organizations not covered by the *Privacy Act* increased to 16 from 15 per cent. Four per cent concerned federal agencies not subject to the Act and 12 per cent concerned organizations outside the federal government. For example, an Ontario government employee wanted to know if her agency could ask female staff whether they planned to become pregnant during the coming budgetary year. She was referred to the Ontario Privacy Commissioner. (A similar request by a federal agency would contravene the federal act.)

The number of misdirected applications remained fairly steady at seven per cent compared to eight per cent last year. The office forwarded these applications to the proper department. Six per cent of calls had nothing to do with the Commissioner's mandate and, whenever possible, were referred elsewhere.

The office's main switchboard (which is shared with the office of the Information Commissioner) redirected 8254 calls to Reference Canada offices across the country. The offices have revised their listings in the blue pages of telephone directories to better explain their mandates. But the combination of "information" in the title and a national toll-free line still prompts many totally unrelated (and expensive) calls.

Compliance Directorate

A seven-year retrospective

Since the *Privacy Act* came into effect on July 1, 1983, 27 government institutions have been audited for general compliance with the Act. In addition, the legitimacy of exempt personal information banks was audited in 11 institutions and more than 16 incidents of possible loss or theft of personal information have been investigated.

Ensuring compliance with the Act has meant breaking new ground with a unique new breed of professional—a hybrid of investigator, auditor, records manager and EDP specialist—the privacy auditor.

Compliance audit is an old and a new subject. What began as the essence of audit work, at the dawn of the 20th century evolved through operational audits, systems-based audits, value for money audits and the ubiquitous comprehensive audit.

However, the day-to-day tools of the traditional auditor cannot assess whether a department's information handling procedures comply with the law. This is so because traditional audit methodology and tools are oriented almost exclusively towards auditing volume and dollar value, not to determining compliance with a set of attributes.

Since the Act came into force, the tools and methodologies have been developed to assist in the audit of massive personal information banks to determine where to expend the scarce audit resources for the greatest good. Vehicles have been put in place to explore and assess the intricacies of the relationship of sections 7 and 8 of the Act as they relate to the security of information systems.

Where today's general auditor uses dollar-unit sampling techniques and utilities, the compliance auditor was left with locally developed questionnaires, a best-guess value for file sampling and a high level guide for the audit of compliance with the *Privacy Act.*

A first step in auditing for privacy meant determining that personal information is:

*collected only when authorized by a specific program or activity;

*kept as long as it serves its original purpose and long enough to allow the subject reasonable access;

*used only for the purpose for which it was collected or for a consistent use;

*disclosed to other parties only when permitted by the *Privacy Act;*

*disposed of at the end of its useful life in accordance with National Archives standards;

*protected according to the government security policy.

The object of the audit for compliance with the *Privacy Act* is to determine whether these six attributes have been accorded to the personal information held in the systems of those institutions subject to the Act. To make this determination requires the use of a tool to locate a statistically significant sample size from personal information banks which may hold as few as a couple of dozen records to as many as several million and then to identify the individual records for the auditor to review.

The first such automated program was developed, tried and field tested in the office of the Privacy Commissioner. It is used today in all audits conducted by the office and is a cornerstone in the methodology developed for use by Commission staff and those institutions which perform their own compliance audits. The program has been successfully employed to audit all types of holdings, from small manual information banks to massive automated relational data bases.

The second step was to develop an automated analytical matrix of criteria to determine the relative audit risk for all of the institutions subject to the Act. Using data derived from a profile questionnaire sent to all institutions in 1986, a computer based model was generated which permitted the Commissioner to assign audit projects based upon demonstrable criteria and not simply the best personal guess. Data for the model are now collected on an annual basis and upgrades allow it to change with the situations.

The third step was to develop and document the methodology so new staff could take advantage of the lessons learned and be consistent in working papers, reports and audit activities. Development of the methodology began early in the process and continues.

The latest step is to integrate the lessons learned and the tools developed with the task of auditing the latest generation of information handling systems and to review and evaluate the security implications of the new technology as it is applied to personal information.

The task is daunting but not without its success. The office has established new relationships with agencies responsible for policy and enforcement such as Treasury Board, the Communications Security Establishment and the RCMP—agencies with expertise in information policy and technology. As well, new colleagues are being found in provincial governments, private enterprise and associations of concerned professionals like the Canadian Information Processing Society, the Information Systems Security Association and the Institute of Internal Auditors.

Four major departments were examined in the first full year of application of new audit method and tools. The next year, six complete audits were done. The past year has witnessed the completion of 14 audits and five incident investigations. Future years will see a consolidation of effort in the largest of the institutions which possess the most sensitive personal information in the most advanced computer systems.

The major lesson to be learned from the Commissioner's auditing experience is that the name of the game is not "gotcha". It is a joint effort that will make privacy compliance a reality.

Without sharing experiences and knowledge and without participating in joint audits, the pursuit of compliance with the *Privacy Act* will remain a one-sided enforcement nightmare. True compliance will be achieved only when institutions, federal, provincial or private recognize the need for and benefits from a set of fair information practices.

During the year the unit audited the Canadian Cultural Properties Review Board, Canadian Patents and Development Limited, Export Development Corporation, Health and Welfare Canada (Medical Services Branch, Income Security Programs and Personnel Administration Branch), International Development Research Centre, Law Reform Commission of Canada, Public Service Staff Relations Board, Security Intelligence Review Committee, Social Sciences and Humanities Research Council and Supply and Services Canada.

What was found

Individual department audits reveal substantially the same weaknesses as those discussed in previous reports. Lack of awareness of the *Privacy Act* remains a major concern. Federal employees often do not know their privacy rights or those of their clients, nor are they aware of the impact the Act has on their day-to-day handling of personal information. The result could be inadequate protection and improper disclosure of clients' personal data. More resources for privacy training would reap dividends for individual departments and the government as a whole.

Personal information collections are often not accurately or completely described in the *Personal Information Index*, making it difficult—if not impossible—for applicants to know information exists or to find the appropriate bank to access. Occasionally personal information is not even recognized as a discrete collection and, therefore, it is not organized in a systematic enough way to attempt to describe.

Several of the institutions were not adhering to the retention and disposal schedules established for personal information after consultation with National Archives. This can lead to using inaccurate information (because it is out of date) or not having information available for access because it has been disposed of too early. It can also overcrowd the records room—but that is not a privacy problem.

Detailed personnel files are often available to supervisors or other employees who have no need to know details about the individual's charitable donations, family relationships, medical conditions, purchases of savings bonds and conflict-of-interest certification.

Inadequate security of personal information is another recurring refrain. Much of government's resources and attention have been put into providing proper security for information which is classified in the national interest (confidential, secret and top secret). Yet loss of, or unauthorized access to, personal information, while it may not damage the national interest, can have quite devastating effects on individuals. The use of FAX is a case in point. While encryption standards are in place and used for the transmission of information classified in the national interest, sensitive personal information is routinely transmitted without protection.

While recommendations to correct this problem may seem both picayune and costly to departments, the potential of this technology to compromise personal information is something this office takes seriously.

Other seemingly minor, yet potentially disastrous security lapses are also regularly uncovered—computer access codes which are never changed or taped to the display terminal, file cabinet keys left in open desk drawers, inadequate door locks, unsupervised access by cleaning staff, inadequate records kept of who has access to files, sensitive information disposed of in ordinary trash, and so forth. Some of the most common sense precautions most individuals take to protect their personal valuables at home seem to go unheeded in the handling of personal information in the federal workplace.

No institution which this office has audited (and among these must be counted the Commissioner's own office) has an unblemished record of privacy compliance. Neither can any department afford to wait for privacy auditors before carefully examining its information handling practices.

Yet there is an important positive side to the story. Departments have demonstrated a high level of sensitivity to and respect for the *Privacy Act*. No systemic or wilfull breaches of the law have been uncovered. Shortcomings are quickly and willingly rectified. More and more departments are including privacy compliance as a regular part of regularly scheduled internal audits. While 27 audits from an audit population of some 150 institutions may not be an adequate basis for generalization, significant achievements should be acknowledged. The caveat is this—no one should rest on deserved laurels, privacy audits will continue!

Some incident investigations

Accident investigation reports restricted

The Commissioner's office pursued a newspaper report which claimed the Manitoba Public Insurance Corporation (MPIC) had used a Transport Canada accident report to deny compensation to a man injured in a traffic accident.

The *Winnipeg Free Press* described how compensation was denied because a Transport Canada research report which assigned him part of the blame had found its way into MPIC files. Police investigating the accident had found the other vehicle at fault.

Compliance staff determined that the report was part of an ongoing study on fatal traffic accidents done for Transport Canada by local universities. The study analyzes accidents to determine the contributing factors and to measure the effectiveness of a number of new safety devices now required on cars. The reports were never designed to replace, or supplement, local police investigations.

Prior to 1978, the lengthy reports contained substantial personal information which a knowledgeable person could link to a specific event. These reports were available in government libraries. In the case in question, it appeared that a local police officer, alleged to have been related to the victims, had given the report to the insurance corporation.

Though the incident happened before the *Privacy Act* came into force, it focused the office's attention on the availability and use of the reports. The privacy investigation found that the new reports are shorter, contain few personal details and are transferred electronically to national accident files.

Privacy staff reviewed the storage methods of both old and new reports and made a number of recommendations to ensure the privacy of those involved in the accidents. Transport Canada readily agreed to new controls which will limit access to the data and ensure that it is used only for research purposes.

Trade Marks Act prevails

A caller told a privacy investigator that approximately 20,000 "protected" files (the security designation for personal information) were kept in an open office in the commercial lobby of a Hull government office.

When investigators visited the area, occupied by the Trade Mark Registry Office of Consumer and Corporate Affairs (CCA), they found names and addresses of those applying for a registered trade mark. The Act requires that this information be protected.

CCA staff pointed to the *Trade Marks Act* which states clearly that the information "shall be open to public inspection". Since the *Privacy Act* protects personal information against disclosure "subject to any other Act of Parliament", the open storage of the files did not breach the Act. Nevertheless, the investigators identified other physical security problems which were noted by CCA privacy staff. These problems are being corrected.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, informatics and library services.

Finance

A new computerized budget control system was introduced to improve the control and reporting of financial commitments and expenditures.

The Offices' total resources for the 1989-90 fiscal year were $5,856,000 and 75 person-years, an increase of $765,000 and six person-years over 1988-89. Personnel costs of $4,481,351 and professional and special services expenditures of $715,783 accounted for more than 90 per cent of expenditures. The remaining $560,135 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1989 to March 31, 1990*

	Information	Privacy	Corporate Management	Total
Salaries	1,585,156	1,794,669	505,526	3,885,351
Employee Benefit Plan Contributions	243,000	274,000	79,000	596,000
Transportation and Communication	36,925	86,040	130,663	253,628
Information	25,133	36,699	2,394	64,226
Professional and Special Services	595,374	68,916	51,493	715,783
Rentals	—	2,381	10,588	12,969
Purchased Repair and Maintenance	2,185	14,271	4,256	20,712
Utilities, Materials and Supplies	16,064	14,330	37,974	68,368
Acquisition of Machinery and Equipment	31,562	38,933	62,031	132,526
Other Payments	1,474	3,521	2,711	7,706
TOTAL	**$2,536,873**	**2,333,760**	**886,636**	**5,757,269**

*Expenditure figures do not incorporate final year-end adjustments reflected in the Office's 1989-90 Public Accounts.

Personnel

With a net increase of six person-years in 1989-90, the first time appointment of an Assistant Privacy Commissioner and the end of term for an Assistant Information Commissioner, the personnel program was active this year again. Thirty-eight staffing actions, including the appointment of one senior management position, were processed and a review of all Program Management positions was conducted to apply the new classification standards. The offices also underwent a staffing audit by the Public Service Commission.

Administration

Additional office space was obtained to accommodate the growth of the organization as well as anticipated needs.

Informatics

A local area network was implemented in the Privacy Commissioner's office to facilitate expansion of report and text production. Preliminary work has also been undertaken to address major changes to the dated case management system. A requirement study of the Information Commissioner's case management system was undertaken.

The office has also started a new informatics management infrastructure to meet the growing needs of the organization.

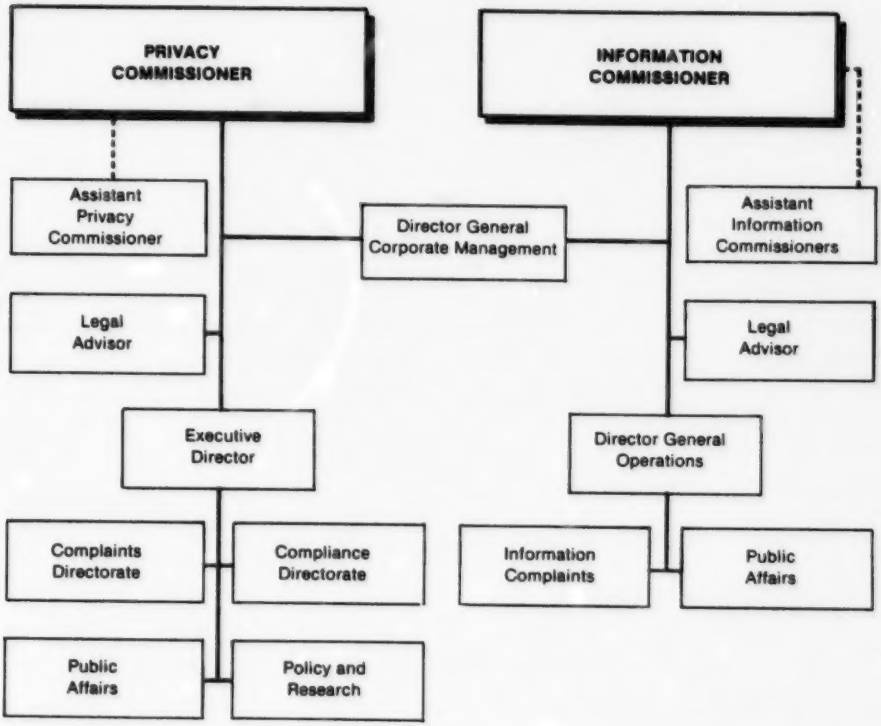
Library

The library supports the programs of both the Information and Privacy Commissioners. It is open to the public.

Among the services offered are the provision of interlibrary loans, manual and automated reference and research, and the maintenance of newspaper clipping files. The library acquires and retains national and international material on all aspects of freedom of information, the right to privacy, data protection and the ombudsman function. Comprehensive collections of annual reports on the administration of the Acts and ombudsman annual reports are also kept.

Automation of library functions is ongoing. Cataloguing of our library collection enables us to provide efficient, quick production of subject bibliographies, lists of periodicals received, and circulation statistics.

Appendix I


PRIVACY COMMISSIONER
INFORMATION COMMISSIONER
Assistant Privacy Commissioner
Director General Corporate Management
Assistant Information Commissioners
Legal Advisor
Legal Advisor
Executive Director
Director General Operations
Complaints Directorate
Compliance Directorate
Information Complaints
Public Affairs
Public Affairs
Policy and Research

Appendix II

Government Institutions Covered by the Act

Advisory Council on the Status of Women

Agricultural Products Board

Agricultural Stabilization Board

Agriculture Canada

Atlantic Canada Opportunities Agency

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Board of Trustees of the Queen Elizabeth II Canadian Fund to Aid in Research on the Diseases of Children

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance Corporation

Canada Employment and Immigration Commission

Canada Labour Relations Board

Canada Lands Company Limited

Canada Mortgage and Housing Corporation

Canada-Newfoundland Offshore Petroleum Board

Canada Nova Scotia Offshore Petroleum Board

Canada Ports Corporation

Canada Post Corporation

Canadian Aviation Safety Board

Canadian Centre for Occupational Health and Safety

Canadian Commercial Corporation

Canadian Cultural Property Export Review Board

Canadian Dairy Commission

Canadian Film Development Corporation (includes Telefilm Canada)

Canadian General Standards Board

Canadian Grain Commission

Canadian Human Rights Commission

Canadian Institute for International Peace and Security

Canadian International Development Agency

Canadian International Trade Tribunal

Canadian Livestock Feed Board

Canadian Museum of Civilization

Canadian Patents and Development Limited

Canadian Pension Commission

Canadian Radio-television and Telecommunications Commission

Canadian Saltfish Corporation

Canadian Security Intelligence Service

Canadian War Museum

The Canadian Wheat Board

Communications, Department of

Consumer and Corporate Affairs Canada

Correctional Service Canada

Defence Construction (1951) Limited

The Director of Soldier Settlement

The Director, The Veterans' Land Act

Economic Council of Canada

Employment and Immigration Canada

Energy, Mines and Resources Canada

Energy Supplies Allocation Board

Environment Canada

Export Development Corporation

External Affairs Canada

Farm Credit Corporation

Federal Business Development Bank

Federal Mortgage Exchange Corporation

Federal-Provincial Relations Office

Finance, Department of

Fisheries and Oceans Canada

Fisheries and Oceans Research Advisory Council

Fisheries Prices Support Board

Freshwater Fish Marketing Corporation

Grain Transportation Agency Administrator, Office of

Great Lakes Pilotage Authority, Ltd.

Hazardous Materials Information Review Commission

Health and Welfare Canada

Historic Sites and Monuments Board of Canada

Immigration and Refugee Board

Indian and Northern Affairs Canada

Industry, Science and Technology Canada

International Development Research Centre

Investment Canada

Jacques Cartier and Champlain Bridges Incorporated

Justice Canada

Labour Canada

Laurentian Pilotage Authority

Law Reform Commission of Canada

Medical Research Council

Merchant Seamen Compensation Board

National Archives of Canada

National Arts Centre Corporation

National Aviation Museum

The National Battlefields Commission

National Capital Commission

National Defence

National Design Council

National Energy Board

National Farm Products Marketing Council

National Film Board

National Gallery of Canada

National Library

National Museum of Natural Sciences

National Museum of Science and Technology

National Parole Board

National Parole Service

National Postal Museum

National Research Council of Canada

National Transportation Agency (formerly Canadian Transport Commission)

Natural Sciences and Engineering Research Council

Northern Canada Power Commission

Northern Pipeline Agency

Northwest Territories Water Board

Office of the Auditor General

Office of the Chief Electoral Officer

Office of the Commissioner of Official Languages

Office of the Comptroller General

Office of the Coordinator, Status of Women

Office of the Correctional Investigator

Office of the Custodian of Enemy Property

Office of the Director of Investigation and Research

Office of the Inspector General of the Canadian Security Intelligence Service

Office of the Superintendent of Financial Institutions Canada

Pacific Pilotage Authority

Pension Appeals Board

Petroleum Compensation Board

Petroleum Monitoring Agency

Prairie Farm Rehabilitation Administration

Privatization and Regulatory Affairs

Privy Council Office

Public Service Commission

Public Service Staff Relations Board

Public Works Canada

Regional Development Incentives Board

Revenue Canada

Royal Canadian Mint

Royal Canadian Mounted Police

Royal Canadian Mounted Police External Review Committee

RCMP Public Complaints Commissioner

The St. Lawrence Seaway Authority

Science Council of Canada

The Seaway International Bridge Corporation, Ltd.

Secretary of State

Security Intelligence Review Committee

Social Sciences and Humanities Research Council

Solicitor General Canada

Standards Council of Canada

Statistics Canada

Statute Revision Commission

Supply and Services Canada

Transport Canada

Treasury Board Secretariat

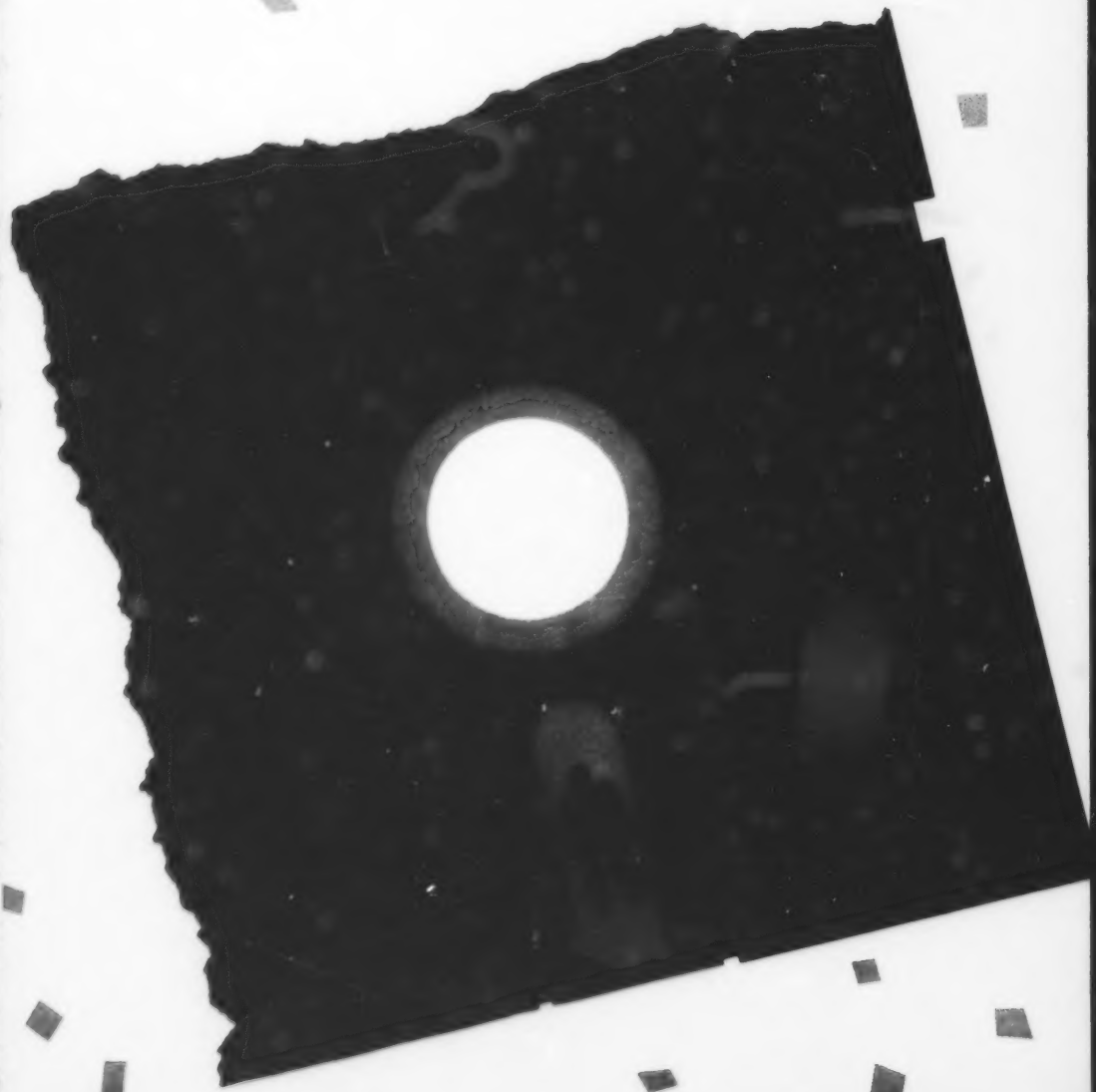
Veterans' Affairs Canada

Veterans' Appeal Board

Yukon Territory Water Board

Commissaire à la protection de la vie privée

Rapport annuel 1989-90



Rapport annuel du Commissaire à la protection de la vie privée 1989-90

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410
1-800-267-0441
Télec. (613) 995-1501

© Ministre des Approvisionnements et Services Canada 1990

N° de cat. IP30-1/1990

ISBN 0-662-57525-3

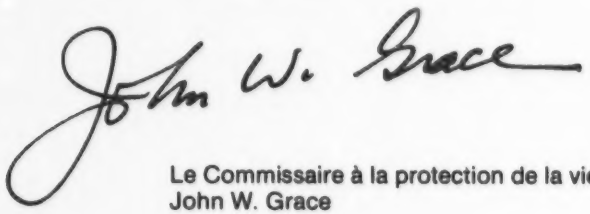
L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 22 mai 1990

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1989 au 31 mars 1990.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

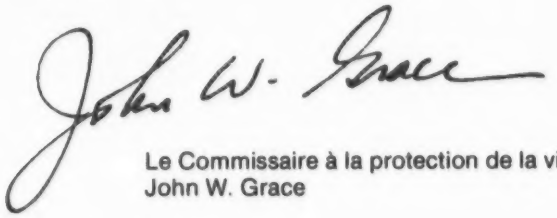
L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 22 mai 1990

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1989 au 31 mars 1990.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

Table des matières

Mandat 1

Le sermon: Un dernier rapport 3

Durant l'année 20
- Ligne ouverte pour les fonctionnaires 20
- L'examen de la Loi sur le SCRS 21
- Encore et toujours, le NAS 23
- Merci, Monsieur le Statisticien 25
- Faites passer 26
- Le dépistage des drogues 27
- Analyse génétique 28
- Les bases de données du CIPC 30
- Les services de contrôle des appels de Bell Canada 32
- Un nouveau fichier inconsultable 33

Direction générale des plaintes 36
- Examen des couplages de données 38
- Aviser le Commissaire 41
- Quelques cas 46
- Demandes générales d'informations 62

Direction générale de l'observation 64
- Rétrospective sur les sept dernières années 64
- Constatations 66
- Quelques incidents 68

Gestion intégrée 70

Annexe I Organigramme 72
Annexe II Institutions assujetties à la Loi 73

Mandat

La *Loi sur la protection des renseignements personnels* donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement :

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
- informe l'individu des fins auxquelles ils sont destinés;
- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si :

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de renseignements donnée dans le Répertoire des renseignements personnels est incorrecte à un quelconque égard;
- la liste donnée dans le Répertoire pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissaire à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Le sermon

"L'avenir n'est plus ce qu'il était."
—William McNeill, professeur d'histoire (ret.) Université de Chicago

Un dernier rapport

Le rapport présenté à la fin d'un mandat de sept ans est pour le Commissaire une occasion unique de déborder le cadre arbitraire d'une période de douze mois pour évaluer la fiche de protection de la vie privée de la nation. Bien sûr, cela peut sembler pompeux… sinon menaçant. Après tout, la *Loi sur la protection des renseignements personnels* oblige seulement le Commissaire à rendre compte au Parlement une fois l'an, et la Loi ne porte que sur l'administration fédérale, et non sur l'ensemble des institutions et des activités du pays.

Pourtant, des commentaires fondés sur sept années d'observation de ce qui se fait (ou ne se fait pas) pour la protection de la vie privée devraient être fondés sur plus que l'expérience des douze derniers mois. Bref, si les observations et les jugements portés dans ce rapport vont parfois au-delà du cadre juridique étroit de la *Loi sur la protection des renseignements personnels*, c'est parce qu'en 1990, le Commissariat à la protection de la vie privée a inévitablement fini par être attiré dans le débat sur des questions nouvelles — et d'une autre envergure — qui entourent désormais la protection de la vie privée.

Cela ne signifie pas pour autant que le Commissaire devrait tenter de s'imposer dans des domaines où il n'a pas compétence. Par contre, en tentant d'éviter le débat et d'ignorer les aspects de protection de la vie privée des tests de dépistage du SIDA ou de l'utilisation de drogues, c'est-à-dire deux des questions les plus délicates de l'heure, il risquerait de voir le Commissariat perdre sa pertinence et son utilité. À cet égard, le phénomène peut-être le plus encourageant de ces sept années est le suivant : qu'on le veuille ou non, à juste titre ou pas, le Commissariat a servi de centre national de ressources sur la protection de la vie privée.

Les demandes de renseignements du public sont passées de 1008 en 1984-1985 à 3447 en 1989-1990. On téléphone et on écrit au Commissariat pour poser toute une gamme de questions, des cas où il faut donner son numéro d'assurance sociale (c'est toujours la question la plus fréquente) aux demandes des médias qui veulent des commentaires sur des points susceptibles d'avoir des implications touchant la protection de la vie privée et aux questions sur les dispositifs affichant le numéro de téléphone de la personne qui appelle à l'écran de notre appareil et même à la proposition du Vérificateur général de créer une ligne directe anonyme qui l'aiderait à dépister les fraudes, en passant par la proposition d'un conseil municipal de distribuer des profils détaillés des criminels libérés.

La protection de la vie privée était naguère une question sociale marginale, une préoccupation ésotérique qui n'intéressait qu'un petit groupe; elle est devenue un problème universel d'actualité. C'est cela qui caractérise l'évolution positive des sept dernières années, et la sensibilisation du public à la protection de la vie privée continue de s'accroître.

Cette sensibilisation s'accroît à chaque nouvelle intrusion de la société — et de l'économie — de l'information dans notre vie privée. L'être humain se porte instinctivement à la défense de sa vie privée pour se protéger contre une technologie tentaculaire qui viole son intimité. Réclamer des mesures de protection de la vie privée, c'est affirmer que le sens de l'humain — que la dignité humaine — devrait l'emporter sur une culture de l'ordinateur qui voudrait régir toutes les transactions et autres opérations enregistrées.

On prétend parfois que la capacité énorme de mémorisation et de saisie de l'ordinateur rend possible une nouvelle Renaissance, une ère de connaissance dans laquelle la machine fera ce que l'homme est incapable de faire, ou qu'il peut faire mais à condition d'accepter d'être accaparé par des tâches répétitives incroyablement aliénantes. Nous nous sommes confortés en nous disant, pour paraphraser un commentateur, que l'information est une ressource renouvelable.

Il est vrai que l'information, contrairement à nos forêts et au pétrole, est renouvelable car des ordinateurs perfectionnés branchés sur des systèmes de communication plus efficaces sont effectivement capables de renouveler l'information et d'en repousser les frontières presque à l'infini. Par contre, la vie privée, elle, n'est pas renouvelable et c'est là le coeur du problème. Une fois qu'un ordinateur indiscret a percé le mur de l'intimité, elle est irrémédiablement perdue, car l'ordinateur n'oublie jamais rien.

Dans une société d'information où le laissez-faire règne, nous ne pouvons même pas contrôler l'utilisation de notre nom. L'avocate américaine spécialiste des communications Anne Branscomb a écrit que la seule façon d'empêcher le trafic de ses renseignements personnels, c'est de devenir ermite, d'avoir un numéro de téléphone confidentiel, de ne jamais payer à crédit et de cesser d'acheter par catalogue. Pourtant, même des précautions aussi peu naturelles n'offrent pas vraiment de garantie.

Tout ce qui limite l'utilisation des banques de données du secteur privé, c'est la conscience des individus qui collectent des renseignements personnels. L'existence de codes volontaires de pratiques équitables est une preuve manifeste que le sens de l'éthique n'est pas perdu. C'est encourageant, et nous en reparlerons plus loin. Néanmoins, la loi ne protège à peu près pas ceux qui décident de ne pas étaler leur vie privée sur la place publique, car la chasse aux renseignements personnels est ouverte, virtuellement sans restrictions.

Le mauvais côté de la médaille

Trop de Canadiens continuent à ignorer l'existence de la *Loi sur la protection des renseignements personnels* et des droits importants qu'elle leur confère. Le fait que 300 000 personnes aient eu recours à la Loi pour demander qu'on leur communique les renseignements qui les concernent contenus dans les dossiers du gouvernement fédéral montre toutefois qu'on la connaît de mieux en mieux et que, lorsqu'on la connaît, on s'en sert. De plus en plus de Canadiens deviennent conscients — même vaguement — du revers de la médaille des technologies nouvelles qui peuvent transformer des êtres humains en «sujets de données» en créant des profils plus ou moins valables fondés sur des renseignements personnels tirés de bases de données en pleine prolifération.

Ces observations pessimistes ne sont pas simplement le fruit du jugement subjectif d'un défenseur professionnel de la vie privée, car l'un après l'autre, les sondages montrent que le public considère cette protection comme l'une des plus grandes priorités de la société moderne.

Comment pouvons-nous espérer protéger notre vie privée contre des satellites espions orbitant à plus de 300 KM d'altitude? Les spécialistes de l'écoute radio n'ont même plus besoin d'avoir accès à un bâtiment pour y installer des capteurs. En outre, la plupart d'entre nous avons des cartes de crédit et des cartes bancaires qui nous relient à de vastes fichiers de renseignements personnels hautement confidentiels, grâce auxquels on sait où nous sommes allés, où nous mangeons, où nous faisons des achats et où nous couchons — et peut-être même avec qui — simplement en comparant des relevés. George Orwell n'aurait jamais imaginé toutes les possibilités modernes du Grand Frère.

Le professeur David Flaherty, de l'Université Western Ontario, est un spécialiste de réputation internationale de la protection des données. Il a été expert-conseil du Comité permanent de la Justice et du Solliciteur général, lorsque celui-ci a étudié la *Loi sur la protection des renseignements personnels*, et il a déjà été cité dans plusieurs de mes rapports annuels précédents. Son dernier livre, intitulé *Protecting Privacy in Surveillance Societies* (Protéger la vie privée dans une société de surveillance) (University of North Carolina Press) contient un passage terriblement inquiétant, dans lequel il soutient que les gens sont de plus en plus susceptibles d'être surveillés par l'intermédiaire des bases de données des secteurs publics et privé, et que ce phénomène est de très mauvais augure pour la qualité de vie de nos sociétés et pour la protection des droits de la personne.

Pour David Flaherty, que reste-t-il du droit qu'on nous fiche la paix, un droit que les tribunaux sont justement en train de définir, quand les bureaux de crédit contrôlent l'information sur le crédit de millions de Canadiens et que l'ordinateur national du Centre d'information de la police canadienne (CIPC) contient peut-être jusqu'à 10 p. 100 des noms de la population adulte du Canada?

Si nous ajoutons à cela les bases de données en pleine expansion du gouvernement fédéral et des gouvernements provinciaux, qui contiennent des renseignements personnels plus ou moins importants selon le cas sur tous ceux qui ont jamais respiré l'air du Canada, et nous arrivons à une situation effarante. Il y a sept ans, le gouvernement fédéral conservait en moyenne 10 à 12 dossiers sur chaque habitant du Canada. Aujourd'hui, ce nombre moyen est bien plus près de 20. L'énormité de ces bases de données est un argument de poids à l'appui de la thèse du professeur Flaherty, qui craint que les sociétés industrielles occidentales soient de plus en plus exposées à devenir des sociétés fondées sur la surveillance, si elles ne le sont pas déjà.

"Il faut avoir un certain respect pour les droits individuels. Nous ne pouvons quand même pas faire subir des tests à tout le monde tout le temps."
—Pat Bowlen, propriétaire des Broncos de Denver

La Charte ... de la vie privée

Sans verser dans l'optimisme béat, il faut reconnaître qu'il y a tout de même des signes encourageants, car les Canadiens sont mieux défendus que beaucoup de leurs contemporains contre les activités de surveillance illimitées. En effet, la *Charte canadienne des droits et libertés* est venue renforcer la *Loi sur la protection des renseignements personnels*, et elle a à ce chapitre dépassé toutes les attentes, en se révélant être une défenderesse étonnamment efficace du droit à la vie privée.

La protection de la vie privée n'est pas un droit expressément garanti par la Charte, et pourtant, la Cour suprême du Canada en a interprété certains articles sans équivoque — et avec force — comme des déclarations favorables à la protection de la vie privée.

Le Commissaire a déjà fait état, dans d'autres rapports annuels, de décisions de la Cour suprême qui ont établi que le «droit à la protection contre les fouilles, les perquisitions ou les saisies abusives» (article 8 de la Charte) protège les particuliers contre les intrusions injustifiées dans leur vie privée. Le 25 janvier 1990, six des sept juges de la Cour qui avaient entendu l'affaire *Mario Duarte c. Sa Majesté la Reine* ont rendu une décision qui a réaffirmé de façon spectaculaire cette interprétation de la Charte.

La Cour devait juger si la Charte donnait à la police le droit de faire enregistrer par un informateur sa conversation avec un présumé trafiquant de drogue, sans la connaissance de ce dernier et sans mandat. La Cour suprême de l'Ontario avait jugé que la police (mais pas les particuliers) était libre d'enregistrer secrètement les conversations privées sans mandat, en autant qu'elle avait la collaboration d'un des interlocuteurs.

Dans ses motifs de jugement pour la majorité des juges, le juge La Forest s'est basé sur des décisions antérieures de la Cour suprême (dont l'une des siennes), en disant que «l'art. 8 vise d'abord et avant tout à assurer le respect de la vie privée». Le paragraphe suivant devrait dissiper tout doute sur l'efficacité avec laquelle la Cour suprême et la Charte peuvent parer à la menace que la technologie représente pour la vie privée :

> La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications restent privées. Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens.

Il est impossible de surestimer l'importance de ce jugement, qui mérite plus d'attention qu'il n'en a reçue.

Ce qui est encourageant, c'est que la décision pose des principes restreignant l'utilisation de la surveillance électronique par la police. Toutefois, le Code pénal n'empêche pas les particuliers d'intercepter les conversations d'autrui, tant que l'un des interlocuteurs y consent. C'est grâce à cette faille que l'utilisation à l'insu des gens de microphones cachés dans des porte-documents et des parapluies, d'antennes paraboliques et de microphones directionnels (comme le «Whisper 2000» annoncé à grand renfort de publicité) continue à proliférer.

Le Code pénal devrait interdire l'interception à notre insu de toutes les conversations privées, en exigeant le consentement de tous les interlocuteurs préalablement à l'interception et/ou à l'enregistrement de leurs communications.

Bref, même s'il ne faudrait pas pour autant cesser d'être vigilant, la décision de la Cour suprême a au moins pour effet de faire du Canada un pays où la vie privée est mieux protégée qu'elle n'aurait pu l'être.

"Dès qu'un journaliste entre dans la pièce, notre vie privée s'arrête où sa liberté d'expression commence."
— Warren Beatty

La presse et la vie privée?

Un autre jugement récent de la Cour suprême mérite d'ailleurs tout autant d'attention.

Dans cette affaire, *Edmonton Journal c. le Procureur général de l'Alberta*, la majorité des juges de la Cour ont conclu que la violation de la vie privée des particuliers était justifiée par l'intérêt public, c'est-à-dire par la liberté de la presse de publier des reportages sur les jugements rendus par les tribunaux.

Cela dit, pour les défenseurs de la vie privée, les motifs de dissidence du juge La Forest (auxquels souscrivaient le juge L'Heureux-Dubé et le juge Sopinka) sont plus significatifs que l'opinion de la majorité. Dans ses décisions antérieures, la Cour suprême avait limité les violations *gouvernementales* de la vie privée des citoyens alors que, dans ses motifs, le juge La Forest a étendu cette protection aux violations non gouvernementales. En l'occurrence, il était disposé à accroître la protection de la Cour parce que, selon lui, «dans notre société, le droit à la vie privée est aussi souvent menacé par d'autres organismes puissants ou influents, contre lesquels l'individu est sans pouvoir.»

D'autres organismes, effectivement. Trois juges de la Cour suprême ont souscrit à la conclusion que «la protection des personnes, de leur famille et des témoins contre l'invasion de leur vie privée constitue ... un motif suffisamment important pour justifier une certaine restriction de la liberté de la presse dans ce contexte». (Il s'agissait d'une affaire matrimoniale.)

Il n'y avait pas de secrets d'État à protéger, et il ne s'agissait pas non plus de protéger la vie privée d'un particulier contre le gouvernement. Dans une affaire à peu près totalement dénuée d'importance pour l'État, une minorité des juges de la Cour était disposée à élargir la portée des interdictions actuelles sur la publication des renseignements personnels. Les trois juges étaient prêts à aller bien au-delà des restrictions applicables aux victimes de voies de fait ou aux jeunes délinquants. Ils étaient prêts à imposer de nouvelles limites à la liberté de la presse parce que la révélation «dans les médias de renseignements personnels relatifs à un individu peut causer un tort incalculable à cette personne et à sa famille».

L'opinion de la majorité, selon laquelle il ne faudrait imposer aucune restriction à la liberté de la presse au sujet des affaires matrimoniales, a retenu toute l'attention des médias. Celle des juges dissidents a été virtuellement passée sous silence, mais à long terme, il se peut fort bien que l'équilibre si difficile entre le droit à la vie privée et la liberté de la presse, qui a été établi dans l'affaire du *Edmonton Journal*, ne soit pas pleinement satisfaisant. Il faudra y revenir, et il est bien possible que les juges La Forest, Sopinka et L'Heureux-Dubé aient finalement gain de cause.

Les dangers que cette affaire présentait pour la liberté de la presse n'étaient que théoriques, après tout; la loi déclarée invalide respectait le principe d'ouverture des tribunaux. La publication du contenu des audiences à l'intention des gens qui s'intéressent vraiment à la procédure ou au droit familial était effectivement autorisée, et l'on pouvait publier toute l'information générale sur la nature de l'affaire. En outre, le journal n'avait pas présenté la moindre preuve que, en 50 ans de publication, la disposition rejetée lui avait jamais interdit de faire un reportage sur une question d'intérêt public.

Il n'y a donc pas lieu de s'étonner que les juges dissidents aient été sceptiques quant à l'importance de l'impact négatif de la loi en question sur la liberté de la presse et des médias et sur le droit du public d'être informé des questions d'intérêt public.

D'un autre côté, le tort causé aux personnes est très réel, comme le dit le juge La Forest :

> Dans les affaires matrimoniales, une personne est amenée à divulguer de nombreux détails sur sa vie privée pour satisfaire aux exigences de l'État quant à la façon dont elle conduit sa vie. Cette intrusion inévitable dans la vie privée de la famille peut, comme nous l'avons déjà vu, avoir un effet considérable non seulement sur les parties elles-mêmes, mais aussi sur les témoins et, ce qui importe davantage, sur les enfants.

De nos jours, la liberté de la presse est bien plus menacée par certains excès des médias eux-mêmes, qui violent la vie privée sans vergogne ni retenue pour servir non pas l'intérêt du public, mais seulement sa curiosité, voire pour le titiller. Au Royaume-Uni, ces excès ont entraîné l'introduction d'un projet de loi qui aurait restreint la publication de renseignements personnels au nom de la protection de la vie privée. Le projet de loi a été retiré, et c'était sage, car son libellé était dangereux. Il reste que cette tentative et l'opinion manifeste de la Cour suprême dans sa décision sur l'affaire du *Edmonton Journal* devraient inciter les médias à faire leur examen de conscience, s'ils en ont une, ne serait-ce que dans leur propre intérêt.

En disant que le droit à la vie privée «occupe un rang élevé dans l'échelle des valeurs à protéger dans une société libre et démocratique», le juge La Forest donne un message plutôt qu'un aphorisme. Et ce message, c'est que le droit à la vie privée est une valeur que les tribunaux — et le public — seront peut-être de plus en plus disposés à préférer même à la liberté de la presse.

Des progrès tangibles

S'il est vrai que le Canada réussit mieux que la plupart des pays à prévenir les intrusions des technologies nouvelles et agressives qui réduiraient l'être humain au statut de sujet de données, il le doit non seulement à une Cour suprême vigilante, mais aussi au Parlement et au Gouvernement lui-même.

Les événements les plus significatifs qui se sont produits depuis sept ans sur la scène de la protection de la vie privée sont, peut-être dans l'ordre, l'examen de la *Loi sur la protection des renseignements personnels* par le Comité permanent de la Justice et du Solliciteur général, la réaction globalement favorable du Gouvernement aux recommandations de ce comité dans *Les nouvelles étapes*, et deux initiatives de principe que le Gouvernement a prises, la première pour limiter l'utilisation du numéro d'assurance sociale (le désormais tristement célèbre NAS) et la seconde pour imposer des mesures de contrôle sur le couplage et l'interconnexion des données informatiques.

Le Commissaire a souligné ces faits dans ses rapports antérieurs, et c'est pourquoi il les reprend dans cette rétrospective. Si le Comité permanent n'avait pas réaffirmé unanimement, avec enthousiasme, les principes de la *Loi sur la protection des renseignements personnels*, et si le Gouvernement n'avait pas accepté les principales recommandations du Comité, la défense de la vie privée aurait risqué l'atrophie.

"Les bureaucrates ambitieux inventent constamment de nouveaux moyens d'utiliser les données à d'autres fins administratives."
David Flaherty, Protecting Privacy in Surveillance Societies

Il est extrêmement important que le Comité ait conclu que la *Loi sur la protection des renseignements personnels* avait su concilier l'intérêt public et les droits individuels. Les deux camps, des chefs de police aux promoteurs des droits civiques, avaient fait preuve d'un certain scepticisme à cet égard, mais le Parlement a dû bien tomber, parce que l'examen de la Loi n'a pas donné lieu au moindre soupçon d'insatisfaction d'un côté ou de l'autre de la barrière idéologique.

L'appui des plus hautes instances du pays a permis à la protection de la vie privée de dépasser le stade de la simple sensibilisation du public, si nécessaire pourtant lorsqu'on amorce une réforme. Il y a sept ans, le droit à la vie privée et la nécessité d'assurer sa protection demeuraient largement des questions abstraites. Aujourd'hui, nous parlons concret, en nous demandant comment mieux contrôler l'utilisation du numéro d'assurance sociale : pourquoi les banques exigent-elles notre NAS? Devons-nous le leur donner pour ouvrir un nouveau compte? Nous nous demandons aussi comment réglementer l'utilisation de tests obligatoires dans la recherche d'un employé «parfait», comment limiter le trafic de renseignements personnels révélant les habitudes de dépenser des gens, des marchandises qu'ils achètent à leurs dons de charité, et comment remettre en question les intrusions des études de marché, des sondages politiques et du recensement, car nous voulons savoir si l'on nous en demande trop, et ce qu'on fait de l'information obtenue.

Même ceux qui ne connaissent pas grand-chose à l'informatique savent ce que les petits ordinateurs bon marché sont capables de faire pour relier et coupler des bases de données afin d'en tirer davantage. Même ceux qui ignorent à peu près tout de la technologie, y compris les protecteurs des données, sont conscients des inconvénients de l'efficience. Les prétendus avantages du couplage, par exemple pour dépister les tricheurs ou les débiteurs, risquent de coûter beaucoup trop cher s'il nous font aboutir à un contrôle systématique des activités des citoyens. Au Canada, le couplage des données informatiques dans les institutions fédérales est désormais régi par des règles sévères dans l'application desquelles le Commissariat joue un rôle. Les Américains, eux, ont même incorporé leurs mécanismes de contrôle équivalents dans une loi fédérale.

"Nous roulons à tombeau ouvert dans la voie de l'extrême gauche, dans un véhicule sans rétroviseur et sans miroirs latéraux."
—Henry Wiseman, Président de la Conférence mondiale sur l'éthique et la technologie, Université de Guelph

Une Loi trop peu connue

Ces sept dernières années, la protection de la vie privée n'est pas restée statique, car les dangers et les moyens de défense ont beaucoup évolué. L'impact de la *Loi sur la protection des renseignements personnels* sur le public, le gouvernement et la fonction publique est désormais irréversible. En sept ans, près de 300 000 personnes (et ces données sont celles du Conseil du Trésor et non du Commissariat) se sont prévalues de la Loi pour demander les renseignements personnels que le gouvernement fédéral avait sur leur compte. C'est déjà étonnant, mais combien de gens auraient fait de même si la *Loi sur la protection des renseignements personnels* était mieux connue?

Le fait reste qu'après tous les discours et tous les rapports du Commissaire, trop peu de Canadiens sont conscients de leurs droits en la matière. Même les fonctionnaires ne connaissent pas encore les droits et les responsabilités qui leur sont dévolus par la Loi. Ce n'est pas là un jugement subjectif : c'est la constatation qui revient le plus souvent dans les vérifications réalisées par le Commissariat.

Et pourtant, il suffit de poser la question à n'importe quel cadre supérieur de la fonction publique (voire à n'importe quel fonctionnaire aspirant à devenir un cadre supérieur) pour constater que ces gens connaissent la *Loi sur la protection des renseignements personnels* ... presque aussi bien que la *Loi sur les langues officielles*. Le droit à la vie privée fait désormais partie de la conscience collective de la fonction publique.

Il suffit pour le confirmer de se rappeler les trois importantes initiatives suivantes, prises au cours de la dernière année.

La Défense nationale permet maintenant aux membres des Forces armées canadiennes d'avoir accès à leur rapport d'appréciation du rendement courant et les informe de leur position sur les listes de sélection au mérite sans qu'ils soient obligés d'en faire la demande officielle en vertu de la *Loi sur la protection des renseignements personnels*.

Approvisionnements et Services a adopté une politique rigoureuse pour veiller à ce que les envois postaux du gouvernement respectent la Loi. Pour sa part, le Conseil du Trésor a envoyé à tous les ministères des lignes directrices sur l'utilisation de leurs listes de distribution postale.

Emploi et Immigration, Industrie, Sciences et Technologie et le Service canadien du renseignement de sécurité comptent parmi les ministères et organismes qui font des vérifications internes pour savoir dans quelle mesure ils respectent la *Loi sur la protection des renseignements personnels*.

Il existe désormais aux échelons les plus élevés de la fonction publique un sentiment d'acceptation et de respect des principes du droit à la vie privée. C'est une généralisation qui peut sembler étonnante, mais il faut souligner un fait frappant : en sept ans, le Commissaire n'a jamais été contraint d'utiliser son arme ultime, c'est-à-dire d'amener une institution gouvernementale devant la Cour fédérale. Bien sûr, certains cas n'ont été réglés qu'à la porte du tribunal, mais c'étaient de rares exceptions. Le point crucial demeure : en fin de compte, on n'a jamais fait fi d'une recommandation du Commissaire.

Bien entendu, le Parlement a nommé un défenseur de la vie privée précisément pour qu'il négocie les différends et qu'il évite le recours aux tribunaux, qui auraient été les premiers à dire que leur charge de travail était déjà écrasante et qu'ils n'avaient vraiment pas besoin d'être appelés à trancher ces différends-là.

Cette absence de recours judiciaire vaut la peine d'être signalée, car tout se fait à deux. À la fin de son mandat, le Commissaire estime qu'il doit absolument féliciter les ministres, sous-ministres, coordonnateurs de la protection de la vie privée et autres gestionnaires d'avoir été si sensibles à la lettre de la Loi et à l'intention des législateurs.

Le désir de respecter la *Loi sur la protection des renseignements personnels* s'est révélé universel, tant chez les organismes détenteurs de certains des renseignements personnels les plus explosifs, comme la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité, que chez ceux qui ont les plus vastes banques d'information, Emploi et Immigration Canada et Revenu Canada, et chez l'institution qui a le moins de dossiers (trois au dernier relevé), l'Office des eaux du Yukon.

Les coordonnateurs: toujours en première ligne

Les rapports de plus en plus étroits qui se sont établis au fil des années entre les coordonnateurs de la protection de la vie privée des différents ministères et organismes et les enquêteurs du Commissariat ont largement contribué à cette absence de recours judiciaires, et leur importance ne saurait être surestimée. Les coordonnateurs les plus occupés sont aujourd'hui aussi rompus à la *Loi sur la protection des renseignements personnels* (ou du moins à certains de ses aspects) que les enquêteurs du Commissariat eux-mêmes. Tous ces coordonnateurs ont en commun un réservoir croissant de connaissances et de précédents, et leur compétence les rend plus utiles encore au ministère ou à l'organisme qu'ils servent, surtout à mesure que la complexité des affaires s'accroît.

En fait, les coordonnateurs, et surtout ceux des grandes institutions, sont devenus de véritables spécialistes de la protection de la vie privée. Ils n'ont pas la tâche facile, car ils doivent concilier leur loyauté pour leur institution d'attache et leur devoir de faire respecter la *Loi sur la protection des renseignements personnels*. Pour résoudre ce dilemme, il leur faut parfois un courage à toute épreuve.

Les ministères éclairés donnent désormais à leurs coordonnateurs le statut que leurs responsabilités méritent. L'an dernier, la coordonnatrice des Anciens combattants a donné des séances d'information dans tous les bureaux régionaux du Ministère. Son rôle de formatrice et son budget de déplacements de 17 000 $ témoignent bien de l'importance que les Anciens combattants attachent à la *Loi sur la protection des renseignements personnels*.

Et la tâche n'est pas finie ...

Voilà pour le côté positif.

Dans un bilan, il faut aussi faire état du côté négatif, car certains de nos déboires ont été plus graves encore que la plus spectaculaire des violations de la vie privée, notre Tchernobyl, le vol des données fiscales concernant 16 millions de Canadiens dans un bureau de Revenu Canada, à Toronto. Cet incident a plus contribué que tous les discours du Commissaire à faire comprendre toute la vulnérabilité des banques de données et à faire reconnaître la nécessité de mesures de protection.

Néanmoins, même après avoir souligné tous les acquis, il reste que trop de fonctionnaires fédéraux persistent dans une ignorance béate du droit à la vie privée et de leur responsabilité de le protéger. Après sept ans, aucun fonctionnaire fédéral ne devrait plus ignorer l'existence de la *Loi sur la protection des renseignements personnels*. Et pourtant, chaque fois que les enquêteurs de la Direction générale de l'observation font une vérification, ils découvrent un peu partout la même sempiternelle rengaine, la même ignorance, pas chez les cadres supérieurs, bien sûr, mais quand même à des niveaux où une ignorance pareille est désormais inexcusable. Cette année, le Conseil du Trésor a donné des cours sur la protection de la vie privée à quelque 700 fonctionnaires. C'est un bon début, mais ce n'est quand même qu'un début.

"Pour éviter un désastre, il nous faut non seulement montrer aux gens comment faire, mais aussi les former pour qu'ils aient un contrôle parfait de ce qu'ils font."
—Son Altesse Royale le Prince Charles

Malheureusement, un volet important de la formation, l'audiovisuel, fait encore défaut. Et le Conseil du Trésor, de même que le Commissariat sont obligés de se contenter d'enregistrements d'extraits diffusés à la télévision commerciale. Après sept ans, il est frustrant — et très embarrassant — d'être obligé de dire aux institutions fédérales de s'adresser aux commissaires ontariens et québécois de la protection de la vie privée pour obtenir du matériel pédagogique audiovisuel. En 1990, le Commissariat n'a même pas pu obtenir la modeste somme de 70 000 $ pour son service des Affaires publiques, parce qu'on lui a dit qu'il était «assez bien connu», à en juger d'après le nombre de plaintes qu'il reçoit.

Le Canadien moyen a de bonnes raisons de ne pas connaître la *Loi sur la protection des renseignements personnels*. Le Conseil du Trésor et le Commissariat ont des ressources très limitées pour une éventuelle campagne d'information du public. Les affiches et les brochures qu'on offre dans les bureaux du gouvernement ont un caractère purement symbolique, malgré toutes les bonnes intentions. Une campagne de publicité en bonne et due forme coûterait beaucoup trop cher, et certains prétendent qu'elle serait contre-indiquée, du moins pour un bureau de défenseur des citoyens.

Et pourtant, on se prévaut rarement d'un droit qu'on connaît mal, et ce droit, qui n'en vaut alors guère la peine, risque de disparaître. Mais tout espoir n'est pas perdu. Certains fonctionnaires se font un devoir de faire connaître la Loi au public. Ainsi, une fonctionnaire d'un Centre d'emploi du Canada de la région d'Ottawa a fait publier dans un journal local un article de son cru sur la Loi. C'est une initiative admirable.

Dans ses rapports antérieurs, le Commissaire a parlé de ses déceptions, par exemple du fait que l'intention du gouvernement d'assujettir les sociétés d'État à la *Loi sur la protection des renseignements personnels* a souffert de deux omissions de taille : Air Canada et Petro-Canada semblent échapper complètement à la Loi. En outre, les modifications qu'il faudrait apporter à la Loi tardent à venir, et le secteur privé ne s'empresse guère d'adopter des codes de protection volontaire de la vie privée, en dépit de l'engagement du Canada d'appliquer les lignes directrices que l'Organisation pour la coopération et le développement économiques (OCDE) s'est données à cet égard.

Bref, le Commissaire déplore essentiellement l'inertie de la bureaucratie et les occasions ratées, mais le monde ne partage pas son sentiment d'urgence. Il n'y a d'ailleurs rien là d'étonnant ou de vraiment mauvais. Ce qui risque le plus de décourager un protecteur de la vie privée, les mauvais jours, c'est tout simplement l'ampleur du danger que posent les technologies nouvelles.

Un régime de protection des données peut-il faire autre chose que parer au plus pressé — et au plus évident — dans un monde de micro-ordinateurs dont la capacité de stockage et de transmission s'accroît sans cesse, où les réseaux locaux prolifèrent, où l'on trouve toujours plus de fiches «intelligentes» lisibles à la machine, de disques au laser, de fibres optiques, de couplages d'ordinateurs, de paiements aux points de vente, de bases de données enrichies, de lecture machine, et j'en passe? Comme le disait le professeur James Rule, de l'Université de l'État de New York, «y a-t-il un point au-delà duquel la collecte de données personnelles devient tout simplement excessive, quels que soient les principes qui régissent les systèmes informatiques?»

Il suffit de penser à l'ampleur du défi pour les protecteurs des données qui sont appelés à surveiller l'application d'un régime centralisé de pratiques d'information équitables dans un environnement de plus en plus décentralisé, voire fragmenté. Dans une publication récente, l'OCDE décrivait les effets fonctionnels du changement technologique comme une «trivialisation du traitement des données». Nous pourrions aussi parler de la «démocratisation» de l'accès au traitement des données en raison de la prolifération non seulement des micro-ordinateurs, mais aussi des systèmes experts et des systèmes de microformes, des disques optiques et de la câblotélévision interactive.

Il y a quatre ans, le Commissaire annonçait avec un certain émoi dans son rapport annuel que le gouvernement fédéral possédait environ 6700 micro-ordinateurs, dont quelque 1700 qu'il s'était procurés au cours de 12 mois précédents. Aujourd'hui, ces appareils sont aussi répandus que l'étaient naguère les machines à écrire manuelles. Presque tout le monde semble avoir renoncé à les compter, mais au meilleur de notre connaissance, l'administration fédérale en utiliserait maintenant environ 30 000.

Et les micro-ordinateurs ne font pas que donner accès à de gros ordinateurs; ils sont eux-mêmes assez gros, merci. En outre, il sont capables d'une extraordinaire polyvalence, à tel point que la notion de «dossier» ou de «fichier» est en train de devenir tout à fait désuète. L'OCDE n'a d'ailleurs pas manqué de le signaler dans un autre rapport : «... il n'est plus nécessaire de travailler avec des systèmes de fichiers clairement définis à l'avance, car on peut facilement les adapter pour leur donner de nouvelles configurations».

Les dossiers sont désormais plus difficiles à cerner que le fameux Mouron Rouge : on peut les ouvrir, les fermer, les combiner, les résumer, les faire disparaître et les faire réapparaître sur pression d'un bouton. Le Conseil de l'Europe a conclu à la suite d'une étude que certains des vieux postulats de la protection des données n'étaient plus valables. Les solutions envisagées dans les années 1970 étaient bonnes dans la mesure où on les appliquait au matériel de pointe de l'époque, c'est-à-dire à de gros ordinateurs autonomes ayant des applications précises et capables d'emmagasiner et de traiter des données sur des personnes «identifiées ou identifiables» dans un «fichier» relevant d'un «contrôleur de fichier» identifiable à volonté par une «autorité de supervision». Aujourd'hui, comment le Commissaire, qui joue le rôle «d'autorité de supervision», peut-il avoir la même assurance qu'il a accès à tout le dossier d'une «personne identifiable», quand il est impossible de définir ce qu'est un dossier ou un fichier?

Nous pouvons même nous demander si les fichiers informatiques dispersés sont effectivement des dossiers. Heureusement, les législateurs ont eu la prévoyance de donner à la *Loi sur la protection des renseignements personnels* un sens très large, car ces renseignements sont ceux qui «... quels que soient leur forme et leur support concernent un individu identifiable». La Loi ne fait mention ni de dossiers ni de fichiers. Elle est aussi muette sur les programmes informatiques à utiliser — ou à éviter d'utiliser — pour l'obtention de ces mêmes renseignements.

À cet égard, rien ne prouve que les institutions gouvernementales canadiennes aient contourné la *Loi sur la protection des renseignements personnels* en refusant de donner accès aux renseignements de ce genre s'ils ne sont pas réunis dans un seul dossier ou un seul fichier et clairement identifiés, et c'est tout à leur honneur. Néanmoins, le fait est qu'on peut instantanément trier, extraire, voire détruire des renseignements emmagasinés et dispersés dans des banques informatiques, sur simple pression de quelques boutons. Chaque fois qu'un nouvel ordinateur perfectionné est mis sur le marché, la tentation d'utiliser la technologie pour se soustraire à la Loi devient plus forte, et comment le Commissaire peut-il faire en sorte qu'on y résiste toujours? Quand il n'est plus indispensable de traiter les données dans le contexte d'un système de banques centralisées, l'efficacité des méthodes actuelles de vérification du respect et des règles de la Loi est remise en question. Avec les nouveaux terminaux décentralisés, interactifs et multifonctionnels, les méthodes de vérification actuelles ne suffisent peut-être plus à relever le défi.

Comment pouvons-nous assurer la sécurité des renseignements personnels et continuer à ne les utiliser qu'à leurs fins originales, quand nous savons qu'il est possible de relier n'importe quel terminal à n'importe quel autre par des lignes publiques ou privées, comme un document récent de l'OCDE l'a souligné?

Les principes généraux de la protection des données se sont remarquablement bien maintenus, précisément parce qu'ils sont généraux. Toutes les études aboutissent à la même conclusion. Il reste que la surveillance de l'utilisation de la technologie doit être à la hauteur des merveilleuses capacités des nouvelles générations d'ordinateurs. Autrement, les protecteurs des données n'auront plus qu'à s'arracher les cheveux et à se répandre en lamentations. Tous les commissariats à la protection de la vie privée doivent absolument rester au fait de la technologie, afin d'avoir des garanties raisonnables que leurs spécialistes sont capables de se mesurer aux plus grands de l'informatique.

"Il faudrait interdire la vente des télécopieurs qui n'ont pas de système de protection des données; ils sont aussi dangereux que des voitures sans freins."
—Le professeur Spiros Simitis, Commissaire à la protection des données de l'État de Hesse (Allemagne)

Dans le meilleur des mondes, les créateurs de l'informatique de demain seraient sensibles aux possibilités de surveillance de leurs produits, et demanderaient conseil aux protecteurs des données dès les premières étapes de leur démarche. Le monde réel est hélas tout autre.

La vie privée, dans le secteur privé

Cela dit, les réflexions pessimistes que le Commissaire se fait les jours de grisaille ne devraient pas nous faire désespérer. Les principes généraux de la protection de la vie privée, qui se sont si bien maintenus, peuvent aussi être adaptés à de nouvelles technologies et à une situation évolutive. L'OCDE a récemment souligné que l'approche réglementaire de la protection de la vie privée évolue globalement vers l'adoption de règles régissant divers secteurs d'activité. Cette approche sectorielle signifie que les règles sont adaptées aux besoins particuliers de chaque secteur, par exemple les banques, les télécommunications, les expéditeurs directs, les compagnies aériennes ou les gouvernements.

Les règles valables dans un secteur peuvent se révéler impraticables — ou totalement inefficaces — dans un autre. Il faut désormais des codes assez souples pour relever le défi de la protection de la vie privée afin de pouvoir vendre des codes de protection volontaire à des entrepreneurs indifférents, hostiles ou simplement sceptiques.

Au Canada, nous pouvons encore conserver un certain optimisme, en nous disant que le secteur privé finira bien par s'engager publiquement à adopter des pratiques équitables de traitement des renseignements personnels. Il y a d'ailleurs des progrès, lents mais réels, dans chaque secteur d'activité.

Dans le rapport annuel de l'an dernier, le Commissaire déclarait :

> En l'absence de preuves plus concluantes de l'efficacité de l'autoréglementation, les partisans des codes de protection volontaire des données dans le secteur privé auront de plus en plus de mal à défendre leur point de vue.

En 1989-1990, le Commissaire a eu de longues consultations avec les associations des secteurs du transport aérien, des télécommunications et des banques. Bien que les membres de ces institutions n'aient pas encore été nombreux à adopter des codes de la protection de la vie privée conformes aux lignes directrices de l'OCDE, ils ont exprimé l'intention d'y adhérer.

L'Association canadienne des banquiers avait mis son projet de code de côté depuis quelques années, mais la plupart des banques à charte songent sérieusement à l'adopter aujourd'hui. L'Association canadienne des transports aériens collabore actuellement avec l'Association internationale des transports aériens en vue de l'adoption d'un code de protection des données contenues dans les dossiers des clients, et elle réétudiera les méthodes qu'elle utilise actuellement pour les dossiers de ses employés. Les entreprises membres de Télécom Canada semblent désormais disposées à réunir leurs pratiques déjà très réglementées d'administration des dossiers de leurs clients dans un code de protection des renseignements personnels. Elles réétudient elles aussi leurs pratiques de gestion des dossiers de leurs employés, pour s'assurer de leur conformité avec les lignes directrices de l'OCDE.

Au début de l'année, lors d'une rencontre du Commissaire avec les membres d'une organisation réunissant la plupart des entreprises réglementées par le gouvernement fédéral, ce travail de pionnier a donné des résultats manifestes. Les participants ont été unanimes dans leur appui pour l'adoption de codes de protection volontaire.

"Le village planétaire est très agité."
—Geraldine Kenney-Wallace, Présidente du Conseil des sciences du Canada

Un coup de pouce, s'il vous plaît!

Il reste que les commissaires à la protection de la vie privée ont déjà eu des promesses d'action du secteur privé, et que ces promesses sont restées lettre morte. Bref, même si les mesures prises par ces trois secteurs de compétence fédérale sont assez positives pour que l'approche des codes de protection volontaire de la vie privée semble demeurer viable, les législateurs devraient maintenant donner un bon coup de pouce à toute cette démarche.

Le gouvernement aurait intérêt à envisager une modification à la *Loi sur la protection des renseignements personnels* qui aurait pour effet d'obliger les entreprises relevant de sa compétence à concevoir, mettre en oeuvre et présenter au Commissaire, pour examen, des codes de protection volontaire des renseignements personnels conformes aux lignes directrices de l'OCDE. Il n'est pas nécessaire que le Commissaire ait le pouvoir d'ordonner des changements à ces codes ou qu'il intervienne dans leur mise en oeuvre, mais il devrait continuer à vérifier leur efficacité et, dans la mesure où les expériences se révéleraient insatisfaisantes, à recommander au Parlement des mesures propres à assurer une réglementation plus stricte de la protection de la vie privée.

D'autre part, les tendances à l'autoréglementation sont claires, et pas seulement au Canada. Même en Europe, où divers pays ont commencé par obliger les entreprises du secteur privé à déposer un registre des renseignements personnels qu'elles détenaient chez les commissaires à la protection de la vie privée, les conditions de délivrance des licences sont libéralisées et l'on favorise l'autoréglementation.

Plus près de nous, un bastion de l'entreprise privée détenteur d'énormes masses de renseignements personnels, American Express, vient d'annoncer que la question de la protection de la vie privée revêtira une telle importance dans les années à venir qu'elle compte se faire un promoteur du droit à la vie privée des consommateurs. Un cadre supérieur de l'entreprise a déclaré qu'American Express s'inquiétait de plus en plus de voir des compagnies recueillir des renseignements à une fin donnée pour ensuite les vendre à une autre compagnie sans le consentement de l'intéressé.

American Express a vu ce qui risquait de se produire, et son sondage sur les attitudes des consommateurs a révélé des faits troublants :

1) 90 pour cent des Américains estiment que les compagnies n'en disent pas assez sur leurs pratiques d'utilisation de leurs listes;

2) 80 pour cent des Américains estiment que les compagnies ne devraient pas communiquer des renseignements personnels à d'autres compagnies;

3) plus du tiers des Américains pensent que le gouvernement fédéral devrait réglementer l'utilisation des listes de ce genre aux États-Unis.

Les réactions des Canadiens seraient-elles nettement différentes? Certainement pas.

Si American Express a adopté un code de protection volontaire de la vie privée, ce n'est pas parce que ses dirigeants se sont soudainement dit qu'il fallait protéger la vie privée, comme une fin en soi. Non; ils sont tout simplement convaincus que la protection de la vie privée est une bonne affaire, à l'aube des années 1990. C'est une bonne affaire d'abord parce que, comme American Express l'explique très bien, les compagnies qui respectent la patience et la vie privée de leurs clients s'en porteront mieux dans les années à venir et ensuite parce que la base de données sur les clients peut devenir un instrument destructeur qui sapera la confiance des gens et qui finira par leur faire perdre le contrôle de leur avenir, au profit du gouvernement.

C'est précisément ce message que le Commissaire à la protection de la vie privée a tant prêché. Aujourd'hui, c'est une entreprise incontestablement privée qui le reprend, de sa propre initiative, et cela devrait lui donner plus de poids encore.

Le père : "As-tu été assez sage pour que le Père Noël t'envoie les cadeaux que tu as demandés?"
Le fils : "Il va m'envoyer ce que je veux, je le sais."
Le père : "Comment le sais-tu?"
Le fils : "Parce que mon nom est dans son ordinateur."
—Conversation entendue par le New York Times

Durant l'année

Ligne ouverte pour les fonctionnaires

Cette année, les Canadiens ont eu droit au spectacle peu commun — mais ô combien édifiant — de deux mandataires du Parlement donnant des conseils contradictoires à leurs maîtres.

Tout a commencé quand le Vérificateur général a proposé l'établissement d'une «ligne ouverte» qui aurait servi à recevoir des accusations anonymes de fraude, de gaspillage ou de maladministration. Le Vérificateur général était d'avis qu'en leur garantissant l'anonymat, les gens auraient été encouragés à parler, puisqu'ils auraient été à l'abri des représailles, et qu'il aurait pu en résulter des économies considérables pour les contribuables. Le raisonnement est manifestement louable.

Le Commissaire est néanmoins intervenu, en raison de la responsabilité qui lui est dévolue par la Loi de défendre certains droits, dont celui de savoir quelles accusations portées contre une personne (et par qui) figurent dans les dossiers du gouvernement. Qu'elles soient fondées et bien intentionnées, comme certaines peuvent l'être, ou dénuées de fondement et portées dans le seul but de nuire, comme d'autres peuvent l'être, la justice fondamentale implique que les accusations ne doivent pas être secrètes ou anonymes.

En l'occurrence, le Vérificateur général et le Commissaire prônaient chacun un principe extrêmement important. C'est pour cette raison que le Commissaire est reconnaissant au Comité des comptes publics de l'avoir invité, avec le Vérificateur général, à présenter ses arguments.

Le Commissaire a déclaré que le Vérificateur général ne pouvait pas offrir aux «dénonciateurs», si bien intentionnés soient-ils, la garantie que leur identité ne serait pas révélée, si la Loi n'était pas modifiée : si le bureau du Vérificateur général était un organisme d'enquête au sens de la Loi, les noms de ses informateurs pourraient être protégés, mais ce n'est pas le cas.

Dans son rapport annuel de 1988 au Parlement, le Vérificateur général a proposé que la Loi soit modifiée pour qu'il soit possible de faire ce qu'il préconisait en recommandant sa ligne ouverte.

Bien entendu, garantir l'anonymat aux dénonciateurs pourrait peut-être faire réaliser des économies à l'État, mais il faut se demander quelles seraient les conséquences d'un régime pareil pour les fonctionnaires, aussi bien les syndiqués que les cadres. Ils seraient plongés dans un univers kafkaïen d'accusations et d'accusateurs inconnus, où ils ne sauraient jamais quand et pourquoi les inquisiteurs leur tomberaient dessus.

Si des lois plus strictes s'imposent pour que les dénonciateurs soient à l'abri de représailles, qu'on les adopte, mais l'histoire, et même l'histoire récente, a montré que les gouvernements qui encouragent leurs citoyens à être des informateurs anonymes leur font payer chèrement cette pratique et la paient très cher, eux aussi.

En définitive, c'est le Parlement et non le Commissaire ou le Vérificateur général qui doit décider quand d'autres principes doivent prévaloir sur le droit à la vie privée. Le Comité des comptes publics n'a pas recommandé de mesures en ce sens, et le Vérificateur général n'a pas non plus relancé sa proposition.

L'examen de la *Loi sur le Service canadien du renseignement de sécurité*

En novembre dernier, le Commissaire a présenté un mémoire au comité spécial chargé d'examiner la *Loi sur le Service canadien du renseignement de sécurité*. Les pages suivantes sont presque toutes tirées de ce mémoire.

Les principales institutions qui composent l'appareil de renseignement du Canada, y compris le Service canadien du renseignement de sécurité (SCRS) doivent se conformer à la *Loi sur la protection des renseignements personnels*. Néanmoins, le Parlement a pris soin d'assurer que les droits d'accès à l'information qui sont garantis par cette Loi ne fassent pas obstacle à la protection de la sécurité nationale.

Après six ans, les constatations du Commissaire et les décisions de la Cour fédérale ont bien montré que la Loi qu'il est chargé d'appliquer peut coexister avec celle qui régit le SCRS, même si l'harmonie n'est pas toujours parfaite.

La nature de ses activités appelle le SCRS à prendre des décisions difficiles sur l'opportunité de placer des personnes sous surveillance. Eu égard à la protection des renseignements personnels, la *Loi sur le Service canadien du renseignement de sécurité* fixe au SCRS des lignes de conduite précises dont ne disposait pas son prédécesseur, le Service de sécurité de la GRC, qui lui a légué nombre des problèmes que la *Loi sur la protection des renseignements personnels* lui a posés. La plupart de ces problèmes ont trait à des renseignements recueillis par le service de sécurité de la GRC, et plus particulièrement à la régularité de sa méthode de collecte et à la possibilité de communiquer les renseignements sans porter atteinte à la mission du SCRS.

La solution de ces problèmes ne réside pas, de l'avis du Commissaire, dans la modification de la *Loi sur le Service canadien du renseignement de sécurité*. Il faudrait plutôt détruire au plus vite les renseignements hérités du Service de sécurité de la GRC, qui ont été recueillis selon des méthodes que la *Loi sur le Service canadien du renseignement de sécurité* n'autoriserait pas aujourd'hui. Cette démarche d'examen et de destruction est déjà amorcée, et le Commissaire est persuadé que le SCRS accorde une priorité suffisante à la tâche.

Dans un rapport intitulé *Modification à la Loi*, le Comité de surveillance des activités de renseignement de sécurité (CSRS) recommande ce qui suit :

> « ... que le Parlement examine s'il serait bon de clarifier la question en ajoutant, au paragraphe 39(2) de la *Loi sur le SCRS*, un alinéa précisant que le Comité est habilité à avoir accès à tous les renseignements en possession du Service, indépendamment de toute enquête entreprise par le Commissaire à l'information ou par le Commissaire à la protection de la vie privée.»

Si l'inquiétude du Comité de surveillance devant le refus du SCRS de mettre certains renseignements à sa disposition est compréhensible, il reste que l'article 33 de la Loi exige que les enquêtes menées par le Commissaire soient secrètes. De plus, le paragraphe 33(2) dispose que «nul n'a le droit absolu d'être présent lorsqu'une autre personne présente des observations au Commissaire, ni d'en recevoir communication ou de faire des commentaires à leur sujet».

La modification que le Comité propose l'habiliterait à prendre connaissance des observations présentées au Commissaire par le SCRS et de la correspondance adressée à celui-ci par le Commissaire, ce qui serait manifestement contraire aux dispositions de l'article 33.

Le Commissaire estime que les limites prévues à l'article 33 de la Loi à l'égard du droit du Comité de surveillance de prendre connaissance des documents du SCRS n'entravent pas le Comité dans l'exercice de son mandat. D'un autre côté, il est convaincu que ces limites sont essentielles pour lui permettre de s'acquitter de son propre mandat, et particulièrement pour protéger l'identité des plaignants et pour favoriser la franchise dans le cadre de l'instruction et du règlement des plaintes. En outre, le Parlement a déjà l'assurance qu'un de ses propres mandataires dispose de tous les pouvoirs nécessaires pour vérifier dans quelle mesure le SCRS respecte le droit des Canadiens à une vie privée.

Dans son rapport annuel pour 1988-1989, le Comité de surveillance a fait état des démarches qu'il avait entreprises auprès du SCRS pour obtenir des dossiers ayant fait l'objet d'une plainte au Commissaire, puis d'un recours devant la Cour fédérale du Canada. Il a justifié ces démarches ainsi : «Nous avons voulu nous assurer que le Service n'avait pas, sans motif valable, empêché le Commissaire d'examiner quoi que ce soit».

Le Commissaire sait gré au Comité de son appui, mais juge que cette affirmation témoigne d'une mauvaise compréhension de son rôle et de ses pouvoirs à l'égard du SCRS.

En effet, le Commissaire dispose, pour l'instruction des plaintes contre le SCRS, de pouvoirs étendus comme ceux de pénétrer dans les locaux et de contraindre les témoins à comparaître, à déposer sous serment et à produire toute preuve matérielle jugée utile à l'enquête.

Aux termes de l'article 68 de la Loi, quiconque entrave l'action du Commissaire dans l'exercice de ses pouvoirs et fonctions est coupable d'une infraction et passible d'une amende sur déclaration sommaire de culpabilité. De plus, la Cour fédérale a elle aussi un rôle à jouer pour faire en sorte que le SCRS respecte la Loi. Le Commissaire — ou un plaignant — peut demander à la Cour de réviser une décision du SCRS de refuser la communication de renseignements.

Ce serait sûrement porter à l'extrême la notion de «surveillance» que de prétendre que le Comité doive intervenir pour assurer que le SCRS respecte la Loi dans ses rapports avec le Commissaire à la protection de la vie privée et avec les personnes désireuses d'exercer les droits que leur garantit la Loi. Cela équivaudrait à contrôler le contrôleur et, qui plus est, un contrôleur mandaté par le Parlement lui-même.

Bref, la recommandation en question met en doute l'efficacité du Commissaire et celle de la Cour fédérale, en plus de laisser entendre que le SCRS ne se conforme pas parfaitement à la Loi. Ce sous-entendu est aussi faux que regrettable, compte tenu des efforts admirables que le SCRS a déployés pour respecter et l'esprit, et la lettre de la Loi.

Un contrôle parallèle par le Comité des rapports du SCRS avec le Commissaire desservirait à la fois le SCRS, le Commissaire, la Cour fédérale, le Parlement et le public.

En conséquence, le Commissaire recommande que le paragraphe 39(2) de la *Loi sur le Service canadien du renseignement de sécurité* ne soit pas modifié de manière à conférer au Comité le droit de prendre connaissance de la correspondance échangée entre le SCRS et le Commissaire au sujet d'une enquête effectuée en vertu de la *Loi sur la protection des renseignements personnels*.

Encore et toujours, le NAS

Avant de conclure que la vieille rengaine du NAS est une complainte, il faut (quand même) souligner qu'il y a eu des notes positives cette année. On a beaucoup parlé des commentaires et des suggestions du Commissaire au sujet du NAS, à telle enseigne que le Commissariat est devenu un point de ralliement pour ceux qui sont frustrés par son utilisation plus ou moins justifiée. Par conséquent, le Commissaire reçoit beaucoup d'appels et de lettres déplorant des utilisations du NAS qui échappent totalement à son mandat, la plupart du temps dans le secteur privé.

Plutôt que de dire qu'il n'a pas compétence pour intervenir, le Commissaire a décidé de faire parvenir ces commentaires et ces plaintes à qui de droit, en insistant toujours sur le fait que, s'il n'est pas illégal de demander le NAS, c'est souvent insultant pour les clients. Il en profite pour «vendre» l'idée des codes de protection volontaire aux entreprises privées, en leur laissant entendre qu'en demandant le NAS avec plus de discernement, elles pourraient fort bien améliorer leurs relations publiques.

Les réactions ont été étonnamment positives, notamment chez General Motors, au Conseil canadien des ingénieurs, à l'Université Western Ontario et chez J.B. Marketing, une entreprise d'informatique.

Voici le résumé de quelques-uns de ces cas. Un député fédéral avait envoyé au Commissaire une annonce parue dans une revue destinée aux ingénieurs; pour délivrer une carte Mastercard, on exigeait le NAS. Le directeur général du Conseil des ingénieurs canadiens s'est montré très réceptif aux commentaires du Commissaire sur l'utilisation croissante du NAS comme identificateur national d'office. Il a répondu au Commissaire qu'il reconnaissait qu'exiger le NAS est une mauvaise pratique commerciale, et qu'il ferait en sorte qu'on ne le demande plus dans les annonces de Mastercard. Il devait quand même se demander s'il n'était pas trop tard pour prendre des mesures de protection de la vie privée. À cet égard, il a cité la promesse que le gouvernement avait faite lorsqu'il a créé le NAS, en 1964, en s'engageant à ne l'utiliser qu'aux fins du régime de prestations d'assurance sociale, ce qui l'a amené à presser le gouvernement de donner le bon exemple en n'exigeant pas le NAS des acheteurs d'obligations d'épargne du Canada.

Le Commissaire a reconnu que, pour toute admirable qu'elle soit, la nouvelle politique gouvernementale visant à diminuer l'utilisation par les organismes fédéraux du NAS a été durement éprouvée par les modifications récemment apportées à la *Loi de l'impôt sur le revenu*, mais il a encouragé son correspondant à ne pas se décourager et à continuer à résister aux demandes non justifiées de communication du NAS.

Un autre député avait communiqué avec le Commissariat au sujet d'une annonce dans les journaux d'une carte de client privilégié du programme de location de voitures de GM. Les gens qui voulaient se prévaloir du programme devaient eux aussi révéler leur NAS. Le député considérait cette exigence comme un exemple de l'utilisation abusive du NAS.

Le Commissaire a écrit au président de General Motors, qui lui a répondu que la compagnie avait vu là l'occasion de mettre en pratique l'un de ses principes d'entreprise, à savoir penser d'abord à sa clientèle, et il a ajouté qu'a l'avenir, dans toutes ses annonces contenant une formule de renseignements personnels sur le client, General Motors n'exigerait plus le numéro d'assurance sociale.

Deux universités ont aussi éliminé leur demande de production du NAS. Dans un cas, c'est le protecteur des citoyens de l'Université Western Ontario lui-même qui a réussi à convaincre les administrateurs de l'Université de cesser d'utiliser le NAS pour contrôler la distribution des clés de casiers aux étudiants.

Dans l'autre cas, un étudiant de l'Université Simon Fraser avait contesté l'obligation de révéler son NAS pour prouver qu'il avait droit à un rabais à l'achat d'un logiciel. Le Commissariat s'est renseigné et il a constaté que la demande de production du NAS figurait sur une formule périmée que la compagnie J.B. Marketing avait fournie à l'Université.

J.B. Marketing a déclaré au Commissaire que la demande de production du NAS était restée par inadvertance sur la formule quand la version américaine avait été modifiée. Le service de l'éducation de l'entreprise s'efforce d'informer sa clientèle qu'il n'est pas nécessaire que le NAS soit fourni pour que la commande passe. La compagnie a demandé que le client communique avec son représentant pour régler le problème.

Autrement dit, les problèmes posés par le NAS ne sont pas insolubles, quand on a la volonté de les résoudre et que les clients résistent à son utilisation injustifiée.

Merci, Monsieur le Statisticien en chef

En fin de mandat, une mention spéciale s'impose pour l'engagement tangible à protéger la vie privée dont a fait preuve le Statisticien en chef du Canada. Cet engagement est particulièrement digne de mention, parce que nombre d'exigences de la Loi ne s'appliquent pas aux dossiers statistiques. Néanmoins, le Statisticien en chef a pris l'initiative de consulter le Commissaire sur les aspects de protection de la vie privée des dossiers statistiques.

Les bases de données de Statistique Canada sont utilisées exclusivement à des fins statistiques, de sorte qu'on ne peut pas légalement s'en servir dans un contexte décisionnel quelconque ayant des répercussions directes sur des personnes. Il reste néanmoins possible de compiler des profils détaillés (et potentiellement dommageables) d'individus en extrayant les données voulues. Il s'ensuit que les décisions sur l'établissement et le couplage de masses de renseignements comme celles-là soulèvent des questions de protection de la vie privée.

Pour bien comprendre le problème, il suffit de penser au sondage sur la santé que Statistique Canada se propose de mener à bien de concert avec le ministère de la Santé du Manitoba et l'Institut canadien des recherches avancées. Ce projet couplerait des renseignements limités tirés de la banque de données des Services de santé du Manitoba avec des données de Statistique Canada, dont certaines tirées du recensement de 1986.

Le projet pilote sur la santé de la population manitobaine établirait une base de données statistiques grâce à laquelle le gouvernement manitobain pourrait évaluer ses besoins en services de santé et élaborer diverses politiques en la matière. Bien entendu, d'autres provinces ont exprimé de l'intérêt pour le projet, et l'Ontario l'a appuyé énergiquement.

Ce serait un projet unique, parce qu'il suppose une première, le couplage de données du recensement avec celles d'autres bases de données administratives. Au départ, le couplage devait être fondé sur les codes postaux et non sur les noms ou les adresses, mais les données obtenues (dont Statistique Canada aura le contrôle exclusif) auraient porté sur des personnes identifiables. Les personnes qui ont fourni des données originales n'auraient jamais pu prévoir que l'information qu'ils ont donnée au Manitoba et à Ottawa aurait pu servir à créer des profils détaillés et délicats de tel ou tel Manitobain.

Comme il l'avait déjà fait pour d'autres questions liées à la vie privée, le Statisticien en chef a demandé au Commissaire si l'intérêt public justifiait ce couplage.

Le Commissaire a reconnu tout l'intérêt public du projet pilote, mais, chose plus importante encore, il a conclu qu'il était possible d'atteindre l'objectif recherché sans intrusion dans la vie privée des intéressés. Il a proposé que la vie privée des répondants soit protégée par le retrait des données d'identification personnelles, c'est-à-dire le code postal.

Certains peuvent juger que la Loi pèche en n'imposant pas les mêmes restrictions sur les renseignements personnels utilisés à des fins statistiques que sur les renseignements personnels utilisés à des fins administratives, mais nul ne devrait toutefois douter que, dans la pratique, il y a des moyens de prévenir les risques posés par l'utilisation des données statistiques.

Et nous devons en remercier le Statisticien en chef du Canada.

Faites passer

La fonction de communication des institutions fait rarement l'objet d'un débat passionné, mais le rôle d'un défenseur du citoyen l'oblige à établir un équilibre précaire entre la nécessité d'informer le public de son existence, sans pour autant sembler se créer du travail ou sans risquer de perdre de la crédibilité.

Les défenseurs de droits particuliers, comme le Commissaire à la protection de la vie privée, doivent aussi savoir concilier la défense des principes dont la loi leur a confié la sauvegarde et la nécessité d'être considérés comme suffisamment impartiaux pour jouer le rôle de médiateur. Ce dilemme ne date pas d'hier.

Le Commissaire à la protection de la vie privée n'a pas mandat de dire au public ce qu'il peut ou non faire, contrairement au Commissaire des droits de la personne ou au Commissaire aux langues officielles. Toutefois, comme les contribuables paient la note et comme il fournit un service à «toute personne présente au Canada», il se doit de se faire connaître des contribuables et de leur être accessible, de même qu'il doit leur rendre des comptes.

Le Commissaire n'a pas laissé cette absence de mandat précis l'empêcher d'informer les Canadiens de leurs droits, mais le manque d'argent a limité ses efforts. Le Commissariat fonctionne depuis sept ans, mais de nombreux législateurs, bien des fonctionnaires et, s'il faut en croire les anecdotes, la plupart des Canadiens, ignorent tout de leurs droits à la protection de leur vie privée. Il y a de quoi être déçu, pour le Commissaire, de léguer une situation pareille à son successeur.

Pourtant, les progrès sont indéniables. Par exemple, au cours de la dernière année seulement, le Commissaire et son personnel se sont adressés à plus de 60 auditoires représentant toute la gamme des parties intéressées, le gouvernement, le secteur privé, les syndicats et les universités. Le Commissaire a pressé le secteur privé d'adopter des codes de protection volontaire de la vie privée, à l'occasion de réunions de la Société canadienne des relations publiques, de l'Association canadienne de l'informatique, de la Air Transportation Association of Canada, des employeurs du secteur des transports et des communications réglementés par le gouvernement fédéral et de l'Association canadienne de gestion des enjeux socio-économiques.

Le Commissaire — ou son personnel — s'est adressé notamment aux participants à un séminaire spécial de Statistique Canada organisé pour étudier un couplage éventuel de données des programmes sociaux fédéraux avec les fichiers provinciaux de bien-être social, aux membres du Conseil national mixte, sur les questions de protection de la vie privée des fonctionnaires, aux gestionnaires de dossiers au sujet des nouvelles politiques sur le couplage des données et sur le numéro d'assurance sociale et aux participants aux séminaires sur le droit de l'Université Dalhousie et de l'Université du Nouveau-Brunswick ainsi qu'aux cours de formation offerts aux nouveaux agents du SCRS.

Le Commissariat a distribué sa documentation aux membres de la Canadian Library Association et de l'Association des bibliothécaires professionnels du Québec, aux centres d'Emploi et Immigration Canada dans huit provinces et aux bureaux des députés fédéraux. En outre, les Affaires publiques ont répondu à plus de 1600 demandes pour de la documentation sur la Loi, sur le rôle du Commissaire et sur les répercussions des mesures de protection des données.

Le dépistage des drogues : tout le monde le fait . . .

Dans le rapport de l'an dernier, il a été question des dangers de la biotechnologie pour la vie privée; le Commissaire s'était engagé à suivre l'évolution de ce dossier.

Le Commissariat a mené à bien une importante étude de l'impact des techniques du dépistage des drogues sur la vie privée et sur la *Loi sur la protection des renseignements personnels*; le rapport sera bientôt rendu public.

L'étude a porté notamment sur les limitations scientifiques de l'analyse d'urine, la méthode la plus commune de dépistage des drogues autres que l'alcool.

Les tests de ce genre ne peuvent déterminer ou mesurer le degré d'incapacité du sujet, ni établir si celui-ci utilise actuellement des drogues. Il peut seulement déterminer qu'il en a utilisé, avec un pourcentage d'erreur de 2 à 5 p. 100.

C'est pour cette raison que l'analyse d'urine est un instrument différent de l'alcootest et de l'analyse du sang, car ces deux dernières méthodes peuvent confirmer l'absorption d'alcool ou de drogues et l'incapacité du sujet au moment du test, quand il conduisait un véhicule ou exécutait d'autres tâches à risques. Comme l'analyse d'urine ne peut confirmer que l'utilisation passée de drogues, il est possible que le sujet en ait pris chez lui et que cela n'ait eu aucun effet sur son exécution d'activités à risques.

On invoquera peut-être la *Charte canadienne des droits et libertés* pour empêcher qu'il soit porté atteinte à la liberté d'un individu d'utiliser des substances intoxicantes quand cette utilisation ne pose pas de danger tangible pour la santé ou la sécurité. La Cour supérieure du Québec en a d'ailleurs décidé ainsi dans l'affaire *Dion c. Sa Majesté la Reine* (1986).

L'analyse d'urine fait intrusion dans la vie privée des gens. Elle n'est pas scientifiquement valable pour déterminer si quelqu'un qui s'adonne à des activités à risques utilise des substances susceptibles de modifier son rendement ou se trouve sous leur influence. Et pourtant, les gouvernements et l'entreprise privée semblent bien pressés d'y avoir recours pour protéger le public, trouver l'employé «parfait» ou les deux.

Par exemple, Transports Canada propose des analyses aléatoires obligatoires de l'urine des travailleurs de l'industrie canadienne des transports. En dépit de toutes les inquiétudes que cela inspire au Commissaire, il se doit de féliciter le gouvernement d'avoir à tout le moins amorcé la discussion publique sur cette proposition, notamment en saisissant le Parlement de la question par suite du dépôt d'un projet de loi, car ceci permettra à toutes les parties, dont le Commissaire, de s'exprimer sur des questions aussi délicates que les suivantes:

1. Existe-t-il des preuves de l'existence d'un problème majeur d'utilisation de drogues chez les travailleurs des transports?

2. Existe-t-il des moyens de s'attaquer au problème qui porteraient moins atteinte à la vie privée?

3. Existe-t-il des mécanismes suffisants pour garantir une protection raisonnable de la vie privée? et

4. Quel rôle les exigences américaines de dépistage des drogues dans l'industrie des transports ont-elles joué dans l'établissement de la politique canadienne de dépistage?

La Loi contient des éléments de réponse à ces questions, et le Commissaire a aussi tenté de trouver des solutions dans son étude sur les tests de dépistage des drogues.

Analyse génétique

On consacre une énergie sans précédent aux recherches sur la génétique humaine, en raison de la valeur incalculable de l'information que les gènes recèlent au sujet des individus. Ce domaine de la recherche biomédicale débouche sur d'extraordinaires méthodes de diagnostic, grâce auxquelles des spécialistes pourront détecter plus vite les maladies, les traiter mieux et éviter la transmission des tares héréditaires. L'analyse génétique est aussi en voie de devenir un outil important pour les forces policières, en raison de ses grandes possibilités d'identification pour prouver l'innocence ou la culpabilité des suspects.

Et pourtant, toute médaille a son revers, car les chercheurs tentent de déterminer la fiabilité de l'analyse génétique comme prédicteur du comportement futur, c'est-à-dire de savoir si l'on est prédisposé à être antisocial ou à souffrir de troubles mentaux ou émotionnels. La recherche constante de l'employé «parfait» amène certains spécialistes à se tourner vers l'analyse génétique pour déterminer la possibilité que tel ou tel employé sera en bonne santé (en éliminant ceux qui sont génétiquement prédisposés à souffrir du cancer ou de troubles cardiaques), qu'il sera honnête et stable, et qu'il aura des aptitudes pour le travail envisagé.

L'industrie de l'assurance s'est elle aussi rendu compte de toutes les possibilités des nouvelles techniques génétiques. À une époque où les tests de dépistage du SIDA deviennent obligatoires pour les polices d'assurance-vie excédant un certain montant, l'analyse génétique a d'immenses avantages.

Enfin, la sélection prénatale est une possibilité manifeste, avec tous les dangers de discrimination que cela suppose contre ceux qui ne satisferaient pas aux normes.

Nos lois ont du rattrapage à faire pour couvrir l'évolution rapide de la technologie génétique. D'autres pays nous devancent de loin, et notre lenteur à légiférer nous expose à de grands dangers.

La République fédérale d'Allemagne (RFA) est à la fine pointe des recherches dans ce domaine. Une commission d'enquête du Parlement y a déjà présenté un rapport sur les avantages et les risques de la technologie génétique. Le protecteur fédéral de la vie privée et ses homologues des différents États ont publié des lignes directrices afin de contrer la menace que l'analyse génétique pose pour la vie privée. Les auteurs des deux rapports déposés jusqu'à présent ont conclu que la RFA devrait adopter des lois fédérales très strictes pour contrôler la nouvelle technologie. Ils ont notamment recommandé :

1. la limitation de l'analyse génétique, dans le système judiciaire, à la seule confirmation de l'identité des individus;

2. l'interdiction de l'analyse génétique dans le contexte de l'emploi;

3. l'ajout obligatoire, dans les contrats d'assurance, d'une clause précisant que l'analyse génétique n'est pas indispensable et que les déclarations normales de consentement à la communication de renseignements personnels par les médecins excluent les renseignements obtenus grâce à l'analyse génétique;

4. l'autorisation de l'évaluation génétique prénatale seulement pour déceler les troubles guérissables qui aboutiraient, s'ils n'étaient pas décelés, à miner gravement la santé et le bien-être de l'enfant à naître;

5. la limitation de l'examen génétique des nouveaux-nés au dépistage des tares pouvant être guéries ou à tout le moins contrôlées avec assez de chances de succès par la thérapeutique; et

6. sauf dans le contexte policier, la limitation de l'analyse génétique aux cas où les sujets y consentent en toute liberté et en pleine connaissance de cause.

Des lignes directrices comme celles-là sont un excellent point de départ pour la protection contre les dangers de la technologie génétique. Bien sûr, certaines de ces recommandations n'ont pas encore été discutées à fond, et il est peut-être impossible de légiférer là-dessus, mais le Parlement devrait être conscient de ces questions en évolution rapide pour faire ce qu'il peut le plus tôt possible afin de préparer des propositions législatives sur l'utilisation de l'analyse génétique.

La Commission de réforme du droit de l'Ontario et la toute nouvelle Commission royale d'enquête fédérale sur la technologie de la reproduction se penchent toutes deux sur des questions de plus grande envergure encore dans ce domaine, et elles savent qu'il faudra peut-être réagir aux nouvelles technologies génétiques.

Le Commissaire continuera de suivre de près l'évolution de la situation, du point de vue de la protection de la vie privée, et il tiendra le Parlement au courant.

Les bases de données informatiques du CIPC

Certains des renseignements personnels les plus délicats que détient le gouvernement sont contenus dans les bases de données informatiques administrées par le Centre d'information de la police canadienne (CIPC).

Le système de renseignements informatisés du CIPC comprend quatre grandes bases de données auxquelles les organismes policiers ont accès, et ceux-ci y ajoutent et en tirent sur une base continuelle toute une gamme de renseignements. Selon la GRC, on aurait fait plus de 72 millions d'opérations dans ces bases de données au cours de l'année financière 1987-1988, et plus de 21 millions de ces opérations portaient sur des particuliers.

Le Centre est financé par le gouvernement fédéral et administré par la GRC. Il est dirigé par un comité consultatif composé de représentants des principaux corps de police municipaux et provinciaux (la GRC assure ces services dans huit des dix provinces), du Procureur général de l'Ontario et de celui du Québec. Toutefois, la responsabilité de l'établissement de la politique et des procédures du CIPC est la prérogative du Commissaire de la GRC.

Étant donné qu'une partie des renseignements détenus par le Centre lui vient de sources non fédérales, la question de savoir de qui relèvent les renseignements personnels contenus dans ses bases de données reste à déterminer. Cela dit, il est certain qu'un contrôle efficace s'impose pour la protection des données.

Le CIPC a été créé pour assurer un traitement et un échange plus efficients des renseignements de nature policière. La GRC qualifie son système de moyen de faciliter l'accès partout au pays à l'information de ce genre et d'améliorer la collecte, le stockage et le contrôle des dossiers par les forces policières.

L'accès aux bases de données du Centre est contrôlé en fonction du statut du demandeur, selon que celui-ci représente une force de police fédérale, provinciale ou municipale, une force policière étrangère ou un organisme ayant un mandat limité d'organisme quasi policier (comme Douanes Canada ou Emploi et Immigration).

Les quatres bases de données sont les suivantes :

1. Fichiers de la Banque de données d'enquête : Fichiers sur les personnes portées disparues et recherchées (y compris les enfants portés disparus), les véhicules et les embarcations volés, les crimes majeurs non résolus et les cadavres non identifiés.

2. Fichiers de la Banque de données de l'Identité judiciaire : Fichiers comprenant les casiers judiciaires et le répertoire des noms des criminels.

3. Fichiers de la Banque de renseignements criminels : Fichiers comprenant le Système automatisé de renseignements sur la criminalité (SARC), à accès limité par 27 terminaux contrôlés par les organismes canadiens de renseignements sur les criminels. Le SARC n'a pas d'interfaces avec l'étranger. Les renseignements qu'il contient concernent des individus, des entreprises, des véhicules et d'autres sujets. Le fichier « Focus » contient des renseignements sur les bandes organisées de motards.

4. Fichiers de la Banque de données auxiliaires : Fichiers comprenant les répertoires des propriétaires de véhicules immatriculés et les détenteurs de permis de conduire, ainsi que des renseignements fournis par les services correctionnels fédéraux et provinciaux.

La GRC exploite aussi un cinquième système informatisé, le SRRJ (Système de récupération de renseignements judiciaires), qui ne relève pas du CIPC. Le SRRJ contient des renseignements sur des événements, des sujets, des véhicules et des biens. Il fonctionne selon le principe du recouvrement des frais et il est mis à la disposition des ministères fédéraux et de 12 corps de police municipaux.

Après son examen approfondi de la Loi, le Comité permanent de la Justice et du Solliciteur général a recommandé que le CIPC y soit assujetti et que le Commissaire vérifie ses bases de données pour s'assurer que le droit à la vie privée des Canadiens est convenablement protégé.

Le Gouvernement a rejeté cette recommandation. Il a préféré demander aux organismes policiers participants quel serait le meilleur moyen d'assurer la protection de la vie privée dans ce contexte. Cependant, lorsqu'il constata qu'aucune solution ne serait proposée par ceux-ci, le Commissaire suggéra que la GRC consulte les utilisateurs du CIPC pour voir comment elle pourrait mettre en oeuvre des mesures de contrôle volontaires de ses bases de données afin d'assurer la protection de la vie privée. Il s'agirait d'une politique exhaustive de protection des données, qui régirait la collecte, l'utilisation, la communication et le retrait des renseignements, le tout assorti de procédures d'accès et de correction.

Le Commissaire a fait quatre suggestions.

Premièrement, le volet le plus délicat d'un code volontaire consiste en une procédure acceptable d'accès et de correction. Le Commissaire a pressé la GRC de ne pas se contenter de renvoyer les demandeurs à l'organisme source, mais plutôt d'envisager de leur donner accès à tout le système via un point d'accès unique.

Deuxièmement, il demanda que la politique ne prévoie que quelques exceptions limitées et bien définies, en invitant la GRC à ne pas aller au-delà des exceptions contenues dans les lois ontarienne, québécoise et fédérale de protection de la vie privée.

Troisièmement, il demanda que la politique assure les particuliers que les renseignements incorrects ou incomplets seraient corrigés ou retirés, tant dans le système informatisé que dans les dossiers et fichiers originaux. En cas de litige sur l'exactitude ou le caractère exhaustif des renseignements, il faudrait préciser que ceux-ci ont fait l'objet d'un litige et y faire figurer la version de l'intéressé.

Enfin, le Commissaire pressa la GRC de mettre en place un mécanisme de règlement des différends au sujet des exceptions, des retards et des demandes de correction.

La GRC a répondu favorablement aux suggestions du Commissaire; elle a déjà commencé à appliquer ces principes dans ses propres systèmes, y compris le SRRJ. En outre, elle a présenté les vues du Commissaire au sujet de la protection de la vie privée au comité consultatif du CIPC, qui étudie activement des mesures de contrôle volontaire pour la protection de la vie privée.

Il est trop tôt pour savoir si ces mesures de contrôle volontaire du CIPC ont des perspectives d'avenir. Toutefois, le fait que les organismes policiers sont disposés à étudier les possibilités qui s'offrent à eux permet au Commissaire d'être optimiste et de se dire qu'il est possible de concilier les besoins légitimes des organismes policiers et les droits à la vie privée des particuliers.

Les services de contrôle des appels de Bell Canada

Il a été question dans le rapport annuel de l'an dernier des implications pour la protection de la vie privée d'une demande présentée au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) pour obliger Bell Canada à vendre la base de données de ses annuaires sous forme lisible à la machine. (Au moment d'aller sous presse, le CRTC n'avait pas encore rendu sa décision.)

En 1989-1990, une autre question de protection de la vie privée mettant en cause les services téléphoniques s'est posée.

Cette fois-ci, Bell Canada a demandé au CRTC de l'autoriser à offrir un certain nombre de services, dont un qui aurait permis l'affichage du numéro de téléphone du correspondant qui fait l'appel grâce à un dispositif spécial. Cette proposition soulève une pléthore de difficultés pour la protection de la vie privée. D'une part, le service serait souhaitable, car il protégerait les abonnés contre le harcèlement ou tout simplement contre les appels indésirables, mais d'autre part, il ne serait plus possible de faire un appel téléphonique sans être identifié, et ce serait regrettable.

Le Commissaire a conclu, non sans hésitation, car il est toujours difficile de dire quel aspect de la protection de la vie privée l'emporte sur les autres, que les inconvénients du service proposé l'emportent sur ses avantages. Au départ, il est inacceptable qu'on soit obligé de s'identifier pour se servir du téléphone. Le téléphone est un service public essentiel que les décideurs ne peuvent traiter comme s'il était optionnel.

Par contre, il est dans l'intérêt du public qu'on offre aux abonnés une façon de prévenir les appels indésirables et ceux qui constituent une intrusion dans leur vie privée. Néanmoins, s'il fallait pour y arriver obliger tous les abonnés à renoncer à leur anonymat, ce serait comme invoquer la *Loi sur les mesures de guerre* pour mettre fin à une bagarre de taverne.

À prime abord, le problème n'est peut-être pas insoluble. Il faut se demander s'il n'y a pas une solution de compromis, un moyen de donner aux abonnés les défenses technologiques proposées tout en permettant à ceux qui peuvent prouver qu'ils ont des raisons légitimes de préserver leur anonymat de ne pas se prévaloir du service. D'autres compétences ont par exemple donné aux policiers en mission secrète et à ceux qui viennent en aide aux victimes de la violence familiale la possibilité de ne pas révéler leur numéro de téléphone. Le Commissariat a cherché un compromis de ce genre.

Toutefois, il a bien dû se rendre à l'évidence : le problème est vraiment insoluble. Dans notre société, le droit à la vie privée de l'un ne prévaut pas sur celui de l'autre et ne peut être imposé à son détriment, et nous ne voudrions d'ailleurs pas qu'il en soit ainsi. Les droits et les libertés fondamentales reconnus par la Charte impliquent des droits à la vie privée jalousement gardés.

Pourrions-nous imaginer que la liberté d'expression, d'association ou de croyance ou que le droit à la liberté et à la sécurité auraient encore un sens si notre vie privée n'était pas bien protégée? Certainement pas, et la Cour suprême du Canada l'a d'ailleurs déclaré sans équivoque dans des affaires comme *Sa Majesté la Reine c. Dyment* (1989) et *Mario Duarte c. Sa Majesté la Reine* (1990).

Le droit à la vie privée serait irrémédiablement compromis si chaque appel à un commerçant, à un ministère ou à un organisme gouvernemental, à un organisme social ou à la presse divulguait automatiquement l'identité de l'intéressé. Pour éviter cette perte de contrôle, nous sommes sûrement prêts à tolérer les abus de certains auteurs d'appels anonymes.

Un nouveau fichier inconsultable

La nouvelle que le Service canadien du renseignement de sécurité (SCRS) créera un nouveau fichier inconsultable — avec l'appui du Commissaire — ne saurait se passer d'explication, surtout lorsqu'on songe que le Commissaire a toujours considéré le principe même d'un fichier inconsultable comme contraire à l'esprit de la Loi, bien qu'il en reconnaisse la nécessité dans certaines circonstances très limitées.

L'histoire tumultueuse des remises en question des 20 premiers fichiers inconsultables est relatée dans les rapports annuels antérieurs. Il ne reste plus que trois de ces fichiers, y compris celui de Revenu Canada (Impôt), qui est traité comme un fichier ouvert, et qui perdra bientôt son statut de fichier inconsultable. Le décret d'exemption du fichier de la GRC a récemment été remplacé, parce que les fichiers individuels n'avaient pas été réétudiés, de sorte que le vieux décret n'était plus valide. Le fichier du SCRS a été légalement constitué et il demeure fermé.

La proposition du SCRS de créer un fichier inconsultable ne fait que reconnaître que le fichier SRS/P-PU-010 est déjà dans les faits un fichier fermé. Ce fichier contient des renseignements sur les personnes qui font l'objet d'une surveillance par le SCRS, laquelle est dûment approuvée, ou qui sont entrées en contact avec des personnes ou des groupes surveillés. Le SCRS répond aux demandes de renseignements tirées de ce fichier sans confirmer ou nier l'existence de renseignements personnels. La Loi n'oblige pas les organismes à confirmer que ces renseignements existent, si l'on pourrait raisonnablement s'attendre à ce que leur communication soit refusée en vertu d'autres dispositions de la Loi.

Cette approche signifie simplement qu'il serait préjudiciable aux activités du SCRS que quelqu'un sache s'il est surveillé ou non par lui. Le Commissaire et la Cour fédérale ont tous deux appuyé ce principe dans l'affaire *Jamshid Zanganeh c. le Service canadien du renseignement de sécurité*.

Les renseignements à caractère moins délicat, concernant par exemple des personnes au sujet desquelles l'ancien Service de sécurité de la GRC s'est intéressé, sont contenus dans le fichier SRS/P-PU-015; ils peuvent être divulgués, avec les exceptions qui s'imposent.

À l'heure actuelle, les fichiers sont officiellement ouverts mais effectivement fermés, ce qui risque d'induire le public en erreur et de ternir l'image de la Loi. Il est donc préférable que le SCRS crée officiellement un fichier inconsultable dûment constitué.

Une mesure comme celle-là impose une lourde responsabilité supplémentaire au Commissaire, qui doit s'assurer que le fichier inconsultable ne contiendra que des renseignements à caractère extrêmement délicat. Il ne faudrait surtout pas qu'après avoir autorisé la création d'un fichier pareil, on lui permette de devenir, sans contrôle, un dépôt secret de renseignements personnels. La Loi le reconnaît d'ailleurs (article 36) en donnant au Commissaire le pouvoir de tenir des enquêtes sur ces fichiers et de recommander que les dossiers qu'ils contiennent soient versés dans des fichiers ouverts, de demander à la Cour fédérale d'ordonner le retrait des dossiers en question si le SCRS n'accepte pas sa recommandation et, bien entendu, de signaler tout refus du SCRS d'appliquer ses recommandations.

Dans un cas comme celui-ci, où le SCRS a un fichier officiellement ouvert mais inconsultable dans la pratique, le Commissaire est privé de ses pouvoirs de contrôle et surtout de son droit de demander à la Cour fédérale, en invoquant l'article 43 de la Loi, « ... d'examiner les dossiers versés dans un fichier inconsultable classé comme tel en vertu de l'article 18». La proposition du SCRS de rétablir un fichier inconsultable corrigerait cette anomalie.

Toutefois, s'il faut en juger d'après une déclaration qui accompagnait la proposition de fermeture du fichier, le SCRS a peut-être l'impression qu'en le fermant, il pourra refuser tout accès à l'information sans être obligé de procéder à l'examen des dossiers. Ce n'est pas de cette façon que le Commissaire interprète la Loi. La disposition autorisant la création de fichiers inconsultables est claire: refuser l'accès à un fichier inconsultable n'est pas une obligation mais plutôt une décision discrétionnaire. Peut-être le SCRS pourrait-il expliquer au Commissaire ou aux tribunaux comment il exercera sa discrétion sans examiner les dossiers demandés? Il semblerait pourtant plus logique qu'il réponde à une demande en examinant le dossier demandé, que le fichier soit inconsultable ou pas.

Bref, même si le SCRS n'est peut-être pas forcé de justifier son refus de divulguer le contenu d'un dossier en invoquant une ou plusieurs des neufs exceptions prévues par la Loi, tous ceux qui se voient refuser l'accès à un fichier inconsultable peuvent porter plainte au Commissaire. En pareil cas, les enquêteurs étudieraient les renseignements pertinents et, si ceux-ci n'étaient pas admissibles à être classés dans un fichier inconsultable, le SCRS se verrait demander de les en retirer et de les traiter comme s'ils étaient dans un fichier ouvert.

Quoi qu'il en soit, le Commissaire s'opposera mordicus à ce qu'un fichier quelconque soit déclaré inconsultable si cela devait avoir pour effet de réduire la quantité de renseignements personnels auxquels les particuliers auraient accès autrement en vertu de la Loi.

Toutefois, compte tenu de la nature de la plus grande partie des renseignements déjà contenus dans le fichier 010 et que le SCRS se propose de transférer dans le nouveau fichier inconsultable, le Commissaire est convaincu qu'on pourrait justifier de les garder secrets, que le fichier soit décrété inconsultable ou pas.

La façon honnête de procéder consiste à rendre le fichier inconsultable pour dissiper la confusion sur l'accessibilité des renseignements, tout en mettant en place des mécanismes appropriés pour que ce fichier inconsultable soit utilisé avec discernement.

Direction générale des plaintes

Après quelques années de statistiques des plaintes en dents de scie — adoption d'une nouvelle méthode de décompte en 1986-1987, baisse du nombre de plaintes en 1987-1988 et remontée en flèche l'an dernier — le rapport de cette année ne contient pas de surprises.

Pendant l'année, le Commissariat a reçu 1086 plaintes ce qui représente une augmentation modeste comparativement aux 1039 plaintes de l'an dernier. Les enquêteurs ont réglé 1018 plaintes, dont 559 étaient bien fondées, 410 étaient non fondées et 49 étaient retirées ou abandonées.

Un code de pratique équitable au sujet des renseignements personnels

Une autre tendance s'est maintenue, à savoir l'augmentation constante du nombre de plaintes relatives à des infractions au code de pratique équitable sur les renseignements personnels décrit aux articles 4 à 8 de la Loi. Ce code régit la collecte, l'utilisation, le traitement, le retrait et la sécurité des renseignements personnels dont le gouvernement se sert pour administrer ses programmes. Depuis 1984-1985, le nombre de ces plaintes a plus que quadruplé.

Le nombre de plaintes de ce type à l'endroit de la Société canadienne des postes, par exemple, s'est accru de façon considérable, surtout dans le cas des plaintes touchant la collecte et l'utilisation des renseignements personnels, passées de 12 en 1988-1989 à 61 cette année. Manifestement, les employés de la Société en sont venus à considérer la Loi comme un mécanisme de règlement des conflits de travail. En effet, ils contestent de cette façon la nouvelle politique restrictive de gestion des congés de la Société, qui exige d'eux plus de renseignements personnels qu'auparavant.

Accès refusé

Les plaintes contestant un refus d'accès aux renseignements personnels se classent encore (de peu) au premier rang des types de plaintes. Le Commissariat a constaté cette année une forte augmentation du nombre de plaintes contre Santé et Bien-être social Canada (SBSC), par exemple; bon nombre de ces plaintes sont liées à la question de la propriété des dossiers médicaux et de leur accès pour le patient.

Jusqu'à cette année, SBSC refusait de laisser les patients avoir accès aux renseignements médicaux même les plus anodins, sauf si le médecin traitant y consentait. Le Commissariat a réussi à convaincre le Ministère à n'obtenir le consentement du médecin traitant que dans les cas exceptionnels, ce qui devrait réduire le délai de traitement des demandes et le nombre de refus de communiquer les renseignements.

Délai non respecté

Le nombre de plaintes de ce genre a légèrement augmenté cette année. Le Service correctionnel du Canada (SCC) est le plus grand retardataire, car il totalise 214 ou 50 p. 100 de toutes ces plaintes. Le Commissaire a jugé bien fondées 78 p. 100 des plaintes de ce genre portées contre le SCC. La Défense nationale est au deuxième rang, loin derrière; 85 p. 100 des 80 plaintes concernant des délais qui ont été logées contre elle ont été considérées bien fondées.

Les difficultés éprouvées par ces institutions à respecter le délai de réponse avaient été signalées pour la première fois dans le rapport annuel de 1984-1985.

Les statistiques montrent que le nombre de plaintes visant des retards indus ont tendance à baisser dans l'ensemble de l'administration gouvernementale, mais le SCC n'a pas encore réussi à surmonter ses difficultés à cet égard. En fait, il semble bien que le non respect, par le SCC, des délais imposés par la Loi soit un problème endémique.

Ainsi, le SCC a pris l'habitude de demander des prolongations de délai pour procéder à des consultations avec d'autres institutions gouvernementales, alors que, dans la mesure où le Commissariat a pu le vérifier, ces consultations n'étaient pas indispensables (et n'ont d'ailleurs pas eu lieu).

La Loi pose des difficultés particulières au SCC. Ses plus importants dirigeants ont souvent fait la preuve de leur respect pour l'esprit et la lettre de la Loi, mais il reste qu'en sept ans, le SCC a eu amplement le temps de consacrer les ressources nécessaires à la tâche et de se donner des procédures administratives efficientes. Les détenus dans les établissements correctionnels ont souvent recours à la Loi pour obtenir leurs dossiers, et le SCC sait fort bien que le Parlement a donné aux criminels les mêmes droits que les autres citoyens de se prévaloir de la Loi.

Il semble que le personnel du SCC est tout simplement d'avis que le droit à la vie privée des détenus est le cadet de ses soucis.

Le SCC répond désormais aux demandes en 70 à 80 jours; les interminables délais de sept à huit mois sont donc chose du passé, mais même cette amélioration ne suffit pas pour qu'il respecte le délai de réponse de 30 jours fixé par la Loi. Pour y arriver, il devra repenser sérieusement ses méthodes.

Le ministère de la Défense nationale (MDN) semble pour sa part en train de résoudre ses difficultés. Il continue à faire l'objet de près de la moitié des demandes fondées sur la Loi, surtout en raison de sa politique qui oblige les militaires à présenter une demande officielle en vertu de la Loi pour voir leurs rapports d'évaluation. Le MDN a décidé, tout à son honneur, car il est difficile de renoncer à une politique qu'on a longtemps défendue, de

renoncer à cette exigence pour maintenant répondre aux demandes de ce genre sur une base informelle. Non seulement cette nouvelle procédure fera-t-elle baisser le nombre de plaintes adressées au Commissaire, mais elle pourra aussi réduire *de moitié* le nombre de demandes officielles de communication de renseignements adressées au MDN.

Il a suffi pour arriver à ce résultat d'éliminer une procédure bureaucratique. La nouvelle approche est conforme à l'esprit de la Loi, et elle met un point final aux pressions exercées depuis des années sur le MDN par le Commissaire, voire par des députés fédéraux.

Nouvelles activités

La Direction générale des plaintes s'est lancée cette année dans deux nouvelles activités, à savoir l'évaluation des nouvelles propositions de couplage de données et l'examen des avis fondés sur l'alinéa 8(2)m). Pour plus de détails sur ces avis, voir *Aviser le Commissaire.*

Examen des propositions de couplage de données

La politique gouvernementale de couplage de données est entrée en vigueur au début de l'année 1989-1990. Elle oblige les institutions gouvernementales à prévenir le Commissariat 60 jours à l'avance de toutes les nouvelles propositions de couplage de données constituant des renseignements personnels, afin que le Commissaire puisse prendre la défense de ceux qui pourraient être lésés par le couplage.

Grâce à cette période de 60 jours, le Commissariat est en mesure d'étudier les propositions en fonction des critères suivants :

- l'évaluation des avantages relatifs du couplage par comparaison avec d'autres méthodes;

- la vérification de l'existence d'une relation directe du couplage avec un programme ou une activité de fonctionnement de l'institution;

Plaintes par motifs et résultats

Motifs	Abandonnée	Bien fondée	Bien fondée Résolue	Non fondée	Total
Accès	11	36	137	259	443
Utilisation/Divulgation	11	14	19	28	72
Correction/Annotation	—	—	5	21	26
Délais	27	317	10	68	422
Langue	—	—	1	2	3
Répertoire	—	—	—	1	1
Collecte	—	13	3	13	29
Conservation/Retrait	—	4	—	18	22
TOTAL	**49**	**384**	**175**	**410**	**1018**

*l'examen de la possibilité de recueillir les renseignements directement auprès des personnes intéressées et, en cas d'impossibilité, pourquoi;

*le fondement de la décision d'aviser les intéressés de la nouvelle utilisation des données et, dans le cas contraire, pourquoi;

*la vérification des mesures prises pour que les nouvelles données soient aussi exactes, à jour et complètes que possible;

*l'évaluation de la pertinence d'obtenir le consentement des intéressés au couplage;

*l'établissement du calendrier d'exécution de la proposition;

*l'analyse des coûts et avantages du couplage.

Après cette évaluation, le Commissaire peut présenter au responsable de l'institution des recommandations sur la proposition de couplage. La décision de procéder ou de ne pas procéder au couplage est prise par le ministre responsable et non par le Commissaire. Le Commissaire peut toutefois saisir directement le Parlement des questions comportant à son avis des risques ou problèmes graves ou sérieux.

Dans ce contexte, le Commissariat a examiné un nouveau système conçu par le Secrétariat du Conseil du Trésor pour coordonner les réponses des ministères aux demandes d'accès à l'information. Le nouveau système a suscité des inquiétudes chez ceux qui se prévalent de la *Loi sur l'accès à l'information* et qui craignaient que la quantité de renseignements communiqués s'en trouverait réduite, parce que l'application du système aurait peut-être incité certains ministères enclins à divulguer plus de renseignements que d'autres à limiter leurs réponses.

Le CDAI

Le nouveau système de Coordination des demandes d'accès à l'information (CDAI) ne constitue pas à proprement parler un couplage de données. C'est plutôt un réseau de micro-ordinateurs donnant accès à une base de données centrale sur les demandes d'accès à l'information adressées aux différents ministères. Ceux-ci doivent communiquer à le CDAI des détails sur les demandes d'accès à l'information qui leur sont adressées. Le CDAI sert de point central de référence et de communication pour l'application de la politique gouvernementale d'accès à l'information. Trente-deux ministères y sont reliés.

Le Commissariat a étudié le CDAI pour vérifier s'il serait possible d'extraire de sa base de données des renseignements personnels sur les personnes qui présentent une demande d'accès à l'information. La réponse a été un «non» catégorique, étant donné qu'on n'introduit pas de renseignements personnels dans la base de données. Il est donc impossible de compromettre leur confidentialité. En outre, les demandes sont décrites de telle façon qu'il est très peu probable qu'on puisse même en déduire des identités. Enfin, l'enquêteur a constaté que le système comportait des mécanismes de sécurité aussi complets qu'efficaces. Bref, le CDAI ne met pas en danger la confidentialité des demandes d'accès à l'information.

Le Commissariat est aussi en train d'examiner trois des couplages de données d'Emploi et Immigration Canada (EIC), dans le contexte du suivi de la vérification interne des mécanismes de protection de la vie privée d'EIC, dont il a été question dans le rapport annuel de 1988-1989. Les couplages étudiés sont les suivants : comparaison des fichiers de la Planification de l'emploi avec ceux des prestations d'assurance-chômage, des fichiers de l'immigration avec ceux du Secrétariat d'État et enfin des fichiers des prestations d'assurance-chômage avec ceux du ministère des Services sociaux de la Colombie-Britannique. L'examen n'était pas encore terminé au moment d'aller sous presse.

Enfin, une troisième évaluation d'un couplage éventuel est encore en gestation; elle portera sur les programmes de couplage rendus nécessaires par la nouvelle taxe sur les produits et services (TPS). Par exemple, Revenu Canada prévoit coupler les données de la TPS et de l'impôt sur le revenu. La Loi oblige aussi les particuliers et les entreprises individuelles à s'enregistrer en donnant leur numéro d'assurance sociale au Ministère, qui le considère comme le moyen le plus efficace d'établir des renvois. Le Commissariat attend actuellement de recevoir des détails de cette proposition.

Enfin, les Affaires extérieures ont demandé officieusement au Commissariat d'examiner sa nouvelle base de données sur son personnel; le Ministère voudrait s'en servir pour remplacer plusieurs systèmes autonomes qu'il utilise actuellement. Le Commissaire attend d'avoir plus de détails pour entreprendre son examen.

Déduction des dettes des chèques de subvention

Un journaliste a demandé au Commissaire si le gouvernement fédéral enfreignait la Loi en déduisant les dettes des producteurs agricoles de leurs subventions de victimes de la sécheresse.

Selon le journaliste, Agriculture Canada avait retenu sur ces chèques les sommes dues au titre des prêts pour l'amélioration agricole garantis par le gouvernement fédéral, les dettes contractées au titre des avances de fonds ou du programme spécial pour les grains, l'argent dû à Revenu Canada ou les pensions alimentaires non payées. Dans ces conditions, le journaliste a demandé au Commissaire si Agriculture Canada avait fait un couplage de données pour déterminer les sommes dues et, si c'était le cas, si le Ministère avait respecté la Loi.

Agriculture Canada a déclaré à l'enquêteur que, quand les producteurs demandaient une subvention aux victimes de la sécheresse, ils étaient tenus de comprendre et d'accepter les conditions précisées dans les lignes directrices accompagnant le formulaire de demande et de consentir aussi aux rajustements ou aux remboursements au gouvernement du Canada qui pourraient s'imposer. Les personnes qui présentaient une demande de subvention de ce genre devaient notamment consentir à ce que l'information sur leur exploitation agricole soit communiquée à tout autre ministère ou organisme gouvernemental ou à toute société d'État, ainsi qu'à divers organismes et offices de commercialisation provinciaux.

Manifestement, les producteurs connaissaient les conditions d'octroi de la subvention, ils les avaient acceptées et avaient consenti à ce que toute l'information pertinente soit communiquée. L'enquêteur a de plus constaté qu'Agriculture Canada n'avait pas couplé ses données avec celles des fichiers de Revenu Canada, bien que la subvention d'un des producteurs ait été réduite à la demande de ce dernier Ministère. Enfin, le formulaire de demande contient une disposition prévoyant un rajustement de la subvention en fonction des pensions alimentaires non-payées, mais ce programme n'est pas encore en vigueur.

Le Commissaire a conclu qu'une enquête officielle n'était pas nécessaire, mais il a rappelé à Agriculture Canada l'importance d'aviser le Commissariat de tout projet de couplage de données.

Aviser le Commissaire

Globalement, la Loi interdit aux organismes fédéraux de communiquer des renseignements personnels à quiconque, sauf à la personne concernée. Toutefois, les choses étant ce qu'elles sont, elle admet 13 exceptions, de la communication exigée par subpoena ou par mandat à la communication faite en vue de l'établissement des droits des peuples autochtones ou du règlement de leurs griefs.

Dans deux de ces cas d'exception, l'institution fédérale doit aviser le Commissaire de la divulgation des renseignements. Il s'agit d'abord de l'information communiquée pour des raisons «d'intérêt public» ou à l'avantage de la personne concernée. L'avis permet au Commissaire de déterminer la pertinence d'informer l'individu concerné de la divulgation et, le cas échéant, de contacter celui-ci.

Le deuxième cas d'exception porte sur la communication des renseignements pour des usages compatibles avec les fins auxquelles ils ont été recueillis, mais qui n'ont pas été décrits publiquement dans le *Répertoires des renseignements personnels*. Ces usages jugés compatibles doivent figurer dans l'édition suivante du Répertoire.

Une certaine confusion entoure l'examen par le Commissaire des propositions de communication pour des raisons «d'intérêt public». La Loi est pourtant claire : la détermination que des renseignements personnels constituent des renseignements d'intérêt public incombe au responsable de l'institution fédérale intéressée, c'est-à-dire généralement au Ministre, et non au Commissaire. Celui-ci est avisé de la communication afin de pouvoir en informer la personne sur laquelle portent les renseignements divulgués, s'il le juge approprié. (Il est possible aussi que le législateur ait pensé que les institutions seraient moins empressées d'invoquer «l'intérêt public» si elles étaient tenus d'en aviser chaque fois un défenseur indépendant des droits des citoyens.)

Le Commissaire ne peut empêcher la communication des renseignements ou exiger que certains détails ne soient pas communiqués, pas plus d'ailleurs que la personne intéressée. C'est étrange, surtout lorsqu'on songe que la *Loi sur l'accès à l'information* donne aux tiers le droit d'empêcher la communication de renseignements jusqu'à la Cour suprême. Le Commissaire a déjà soutenu que les citoyens devraient eux aussi pouvoir empêcher une communication injustifiée ou préjudiciable des renseignements personnels qui les concernent.

Dans la pratique, le Commissariat s'est toujours montré disposé à participer à des discussions sur une éventuelle communication; ces discussions amènent parfois l'institution intéressée à repenser son approche. Le Commissaire reste lui-même à l'écart de ces pourparlers, car il doit protéger son indépendance afin de pouvoir enquêter en toute impartialité si quelqu'un se plaint que la communication des renseignements était injustifiée.

Les exemples suivants sont tirés des 32 cas où le Commissaire a reçu un avis pendant la dernière année.

Communication des rapports d'évaluation d'un médecin

Le ministère de la Défense nationale a informé le Commissaire qu'il voulait communiquer les rapports d'évaluation d'un médecin militaire à un Collège provincial des médecins.

Avant de le relever de ses fonctions, les Forces avaient procédé à une vérification du service médical que dirigeait ce médecin, ainsi qu'à une évaluation de sa compétence personnelle. Compte tenu du renvoi et des normes de pratique de l'intéressé, le Collège avait demandé à voir les rapports en question pour être plus en mesure d'évaluer sa compétence professionnelle. Le Collège tenait, dans l'intérêt du public, à ce qu'un médecin détenteur d'une licence ait un minimum de compétence médicale.

Le Commissaire a informé le médecin de la communication des documents.

Communication des dossiers de Canadiens d'origine japonaise

Le Secrétariat du redressement des Canadiens japonais a demandé aux Archives nationales de lui communiquer les renseignements provenant du bureau de Vancouver du séquestre (biens ennemis).

Ces renseignements portent sur les Canadiens d'origine japonaise internés pendant la Deuxième Guerre mondiale. Ils comprennent notamment les procès-verbaux des comités consultatifs sur la disposition des biens des intéressés, de la correspondance, des registres contenant des inscriptions sur les sommes d'argent gardées en fiducie et sur les biens immeubles, ainsi que des dossiers d'opérations commerciales.

Le Secrétariat était d'avis (tout comme les Archives) que la communication de ces renseignements était justifiée pour des raisons d'intérêt public, car elle allait aider le gouvernement à dédommager environ 12 000 Canadiens d'origine japonaise admissibles.

Le Commissaire a jugé qu'il n'avait aucune raison de s'opposer à la communication des renseignements.

Communication des rapports portant sur l'évasion de deux détenus

Le Service correctionnel du Canada (SCC) a avisé le Commissaire à deux reprises qu'il comptait rendre publics des rapports détaillés sur des évasions de criminels détenus dans des établissements fédéraux.

Les auteurs indépendants de ces rapports avaient décrit des circonstances entourant l'évasion de deux détenus condamnés pour meurtre; les documents contenaient des noms et divers renseignements personnels sur des fonctionnaires fédéraux et sur des particuliers.

Le premier rapport portait sur le cas d'Allan Légère, qui s'était évadé pendant qu'il était sous traitement à l'hôpital Georges-Dumont, à Moncton, au Nouveau-Brunswick. Il était considéré comme dangereux, et on le soupçonnait d'avoir commis plusieurs meurtres après son évasion. Les habitants de la région étaient très inquiets jusqu'à ce qu'il soit repris.

Le deuxième rapport a trait aux circonstances qui ont entouré l'évasion de Daniel Gingras, qui était détenu à l'établissement d'Edmonton, et qui avait profité d'une permission de sortie d'une journée avec escorte pour s'enfuir à bord du véhicule dans lequel il avait pris place avec son gardien, après avoir neutralisé ce dernier. Par la suite, Gingras a été reconnu coupable de deux meurtres commis après son évasion.

Dans les deux cas, le SCC était d'avis que le public avait vraiment intérêt à comprendre ce qui avait mené aux évasions et à savoir que toutes les erreurs de procédure avaient été corrigées.

Le Commissaire a écrit à toutes les personnes nommées dans les rapports pour les informer des conditions de la communication des renseignements, en les invitant à téléphoner au Commissariat pour obtenir des explications sur la procédure.

Une femme cherche à obtenir confirmation de la citoyenneté d'un tiers

Le Secrétariat d'État a avisé le Commissaire qu'il avait l'intention de confirmer la citoyenneté canadienne d'un homme à sa belle-sœur. L'homme, dont l'épouse était décédée, avait quitté le pays et semblait avoir abandonné ses deux filles. L'organisme provincial de protection de la jeunesse avait besoin de ce renseignement pour rendre une décision sur la demande de garde des deux filles par leur tante.

Le Commissaire s'est dit d'accord.

EIC communique des renseignements sur un immigrant

Emploi et Immigration Canada (EIC) a avisé le Commissaire de son intention de communiquer des renseignements à un député fédéral qui faisait pression sur le gouvernement pour faire expulser un ressortissant étranger du Canada.

Le député soutenait que cet étranger ne pouvait être jugé admissible à résider en permanence au Canada, en raison de son appartenance à une certaine organisation. EIC voulait communiquer un certain nombre de détails au député pour le persuader du contraire.

La question était à l'étude quand un journaliste a téléphoné au Commissariat pour savoir si le Commissaire avait approuvé la communication des renseignements. Le député avait apparemment déjà obtenu l'information en question.

Le Commissaire a déclaré à EIC qu'il doutait que la communication des renseignements ait été appropriée. Il a écrit à l'intéressé pour lui donner un aperçu des détails qu'on avait révélés au député et pour l'informer de son droit de porter plainte s'il le désirait.

La vie privée des anciens fonctionnaires

Les fonctionnaires fédéraux ne perdent pas leurs droits à la vie privée lorsqu'ils prennent leur retraite, ce cas-ci l'illustre bien. Approvisionnements et Services Canada (ASC) a téléphoné au Commissariat afin de savoir comment répondre à une demande de communication d'une liste d'agents de communications gouvernementaux à la retraite.

Protection civile Canada voulait avoir cette liste pour entrer en contact avec ces anciens fonctionnaires afin de vérifier s'ils seraient disposés à être sur une liste d'appel pour les cas d'urgence majeure, d'où sa demande des noms et adresses de ces anciens agents à ASC.

Le personnel d'ASC avait rejeté la demande, mais il a téléphoné au Commissariat pour savoir s'il aurait été légalement possible pour ASC d'utiliser sa liste compilée pour l'envoi des chèques de pension de retraite pour contacter lui-même ces retraités.

Après discussion avec le Commissariat, ASC a confirmé son rejet de la demande de Protection civile Canada, en lui suggérant de contacter les agents de communication avant leur retraite.

Origine des plaintes réglées par province et territoire

Terre-Neuve	6
Île-du-Prince-Édouard	7
Nouvelle-Écosse	57
Nouveau-Brunswick	39
Québec	147
Région de la Capitale nationale Québec	1
Région de la Capitale nationale Ontario	102
Ontario	362
Manitoba	58
Saskatchewan	39
Alberta	80
Colombie-Britannique	113
Territoires du Nord-Ouest	2
Yukon	0
Hors Canada	2
Total	1018

Quelques cas

Le carnet de notes d'un superviseur est un dossier du Ministère

Un homme de la région de Toronto s'est plaint que Travaux publics Canada (TPC) avait rejeté sa demande de voir le contenu du carnet de notes que son superviseur tenait sur son compte. Les communications entre les deux hommes étant rompues, le superviseur prenait des notes sur le comportement professionnel du plaignant.

Le plaignant a allégué que le superviseur gardait son carnet de notes sous clé dans son classeur. Quand les autorités de TPC examinèrent le carnet de notes, elles en déclarèrent tout le contenu inconsultable, en disant qu'il concernait une autre personne (le superviseur) à laquelle sa communication pouvait être préjudiciable.

Lorsque les autorités de TPC furent saisies de la plainte, elles affirmèrent que le carnet de notes n'aurait pas dû être examiné du tout, étant donné qu'il était la propriété personnelle du superviseur et qu'il ne relevait pas d'une institution fédérale. Elles ont aussi contesté la compétence du Commissaire de faire enquête sur une plainte concernant une «propriété privée».

Quand le Commissariat a demandé à examiner le carnet de notes, il a constaté que le Ministère pouvait demander au superviseur de le produire n'importe quand (par exemple en réponse à la demande de le consulter en vertu de la Loi) et par conséquent, qu'il relevait donc du Ministère. L'enquête révéla aussi que le superviseur avait commencé à tenir ce carnet après une discussion avec un de ses supérieurs. Le carnet ne contenait que des inscriptions portant sur les allées et venues du plaignant et sur ses activités à son lieu de travail. Le superviseur avait pris des notes dans l'exercice de ses fonctions, et il pouvait s'en servir à des fins professionnelles, notamment pour préparer des évaluations ou pour répondre à des griefs. Par conséquent, le carnet de notes était assujetti à la Loi.

Le carnet renfermait très peu d'informations sur des tiers, et les notes ne pouvaient être considérées comme des renseignements personnels se rapportant au superviseur. Cette constation des enquêteurs a remis en question le refus original du Ministère, que celui-ci avait justifié en disant que les renseignements concernaient d'autres fonctionnaires. Le Ministère avait aussi prétendu que le superviseur avait commencé à tenir le carnet parce qu'il croyait être en danger et qu'il pensait avoir besoin de notes en cas de poursuites judiciaires. Toutefois, le superviseur a déclaré à l'enquêteur qu'il ne croyait pas que la communication du contenu du carnet le mettrait en danger.

Malgré une série de rencontres, le Ministère et le Commissariat n'ont pas réussi à se mettre d'accord pour savoir de qui le carnet de notes relevait. Le Commissariat a continué à s'efforcer de dénouer l'impasse, et, après plusieurs mois de discussions, le Ministère a consenti à remettre au plaignant une photocopie des pages du carnet, après en avoir retiré les renseignements sur d'autres personnes.

Le Commissaire a jugé la plainte bien fondée.

... mais pas les aide-mémoire des commissaires

Dans une autre affaire analogue, le Commissaire a pu établir une distinction subtile entre les renseignements destinés à être utilisés à des fins administratives (comme dans le cas du carnet du superviseur des Travaux publics) et les notes prises comme aide-mémoire par un membre d'un tribunal quasi judiciaire.

Dans ce dernier cas, un ancien fonctionnaire s'était vu refuser l'accès à des notes prises par l'arbitre au cours d'une audience de la Commission des relations de travail dans la fonction publique. L'arbitre entendait l'appel que cet ancien fonctionnaire avait interjeté de son renvoi pour utilisation non autorisée du système téléphonique du gouvernement.

Les arbitres prennent de nombreuses notes pendant les audiences parce que leur contenu n'est pas enregistré et qu'il n'y a pas de transcription des témoignages et des interventions. Leurs notes doivent refléter toute la preuve présentée et toutes les questions soulevées, et pas seulement leurs conclusions. Par la suite, ils rédigent leurs décisions en se reportant à leurs notes, qui sont habituellement détruites une fois la décision rendue publique. Dans le cas qui nous intéresse, les notes n'avaient pas été détruites.

Lorsqu'elle a été saisie de la plainte, la Commission a déclaré que les notes étaient la propriété personnelle de l'arbitre et qu'elles ne relevaient donc pas d'elle, même si elles étaient conservées dans le bureau de l'arbitre. La Commission a cité de la jurisprudence à l'appui de son raisonnement. Toutefois, l'arbitre a accepté, sans préjudice, de laisser l'enquêteur du Commissariat examiner ses 92 pages de notes. Il n'y avait aucun doute que ces renseignements concernaient le plaignant, mais ils ne constituaient en définitive qu'un compte rendu de la preuve présentée à l'audience. Ils ne constituaient pas eux-mêmes un élément de preuve et ils n'avaient pas été utilisés à des fins administratives. Le Commissaire a conclu que les notes ne relevaient donc pas de la Commission et, par conséquent, qu'elles n'étaient pas assujetties à la Loi.

En outre, le Commissaire a souligné que, même si les notes avaient relevé de la Commission, celle-ci aurait pu refuser de les communiquer en vertu d'un autre article de la Loi, qui autorise la non-communication des renseignements si celle-ci peut nuire à l'application d'une loi quelconque. Il a conclu que l'examen des notes de l'arbitre aurait pu nuire à l'application de la Loi et d'autres lois, car il aurait en l'occurrence pu servir à tenter de contourner la décision rendue. Le Commissaire a jugé la plainte non fondée.

Les frais sont à la charge du Ministère

Une plainte a amené le Commissaire à rappeler à Santé et Bien-être social Canada (SBSC) que les frais d'accès aux renseignements personnels étaient à sa charge. La plainte portait sur la réponse donnée par SBSC à la demande d'un homme de la Nouvelle-Écosse qui voulait voir son dossier de demande de pension d'invalidité en vertu du Régime de pensions du Canada. La pension lui avait été refusée.

Le plaignant a déclaré avoir attendu deux mois pour obtenir des renseignements «inutiles», alors que la période de réponse est de 30 jours. Il a dit à l'enquêteur qu'on avait refusé de lui communiquer l'un des deux rapports de médecins sur son cas, en lui disant qu'il ne serait pas dans son intérêt de le voir. Bien que le médecin ait refusé de communiquer le rapport au plaignant, il avait accepté d'en parler avec lui. D'après SBSC, le plaignant allait devoir payer cette consultation.

Cette plainte en apparence toute simple est devenue vraiment embêtante quand SBSC n'a pas répondu à l'avis de plainte et n'a pas retourné les appels téléphoniques du Commissariat. Les difficultés se sont compliquées encore davantage quand l'enquêteur est allé examiner les documents et qu'il a découvert que tout le dossier avait été égaré. La demande de pension d'invalidité, l'appel interjeté de la décision de SBSC et la mention de la demande fondée sur la Loi, tout avait disparu. La Loi n'autorise la non-communication des renseignements médicaux que lorsque le Ministère peut démontrer que la communication serait contraire aux intérêts du requérant. Le personnel de SBSC a admis que cela serait difficile à prouver, étant donné que le dossier avait été perdu. Il a aussi reconnu qu'il n'était pas correct de faire payer par le demandeur une procédure quelconque intentée en vertu de la Loi.

Le plaignant a consulté son médecin, comme on le lui avait proposé, et la consultation ne lui a pas été facturée. Il croit que le médecin a facturé le régime provincial d'assurance-maladie.

Le dossier est encore perdu. Toutefois, SBSC a mis en place de nouvelles procédures d'inscription et de traitement des dossiers personnels et lancé un projet pilote sur un nouveau système de repérage.

Le Commissaire a jugé la plainte sur le long délai de réponse non fondée, étant donné que les ministères peuvent prendre jusqu'à 30 jours de plus pour consulter d'autres parties (en l'occurrence les deux médecins). SBSC a prétendu avoir mis les renseignements à la poste 56 jours après avoir reçu la demande, respectant ainsi le délai de 60 jours. Néanmoins, la plainte portant sur le refus d'accès à l'information était bien fondée, puisque le Commissaire n'a pas pu examiner les renseignements pour déterminer si le refus de les communiquer était justifié. La plainte que certains frais allaient être à la charge du plaignant a été considérée bien fondée, elle aussi.

Une erreur datant de 40 ans a été corrigée

Un Ontarien a écrit au Commissaire, en dernier recours, pour que la Défense nationale lui rembourse ce qu'il prétendait être une dette contractée depuis 40 ans.

Le plaignant avait servi dans l'armée britannique pendant la Deuxième Guerre mondiale et, à ce titre, il avait droit à un indemnité de fin de service. En septembre 1946, le gouvernement britannique l'avait informé que l'indemnité lui serait versée au Canada; il avait demandé par écrit comment le montant serait calculé. L'Amirauté britannique lui avait écrit en novembre de la même année au sujet du «paiement qui lui avait été versé récemment».

Entre-temps, le plaignant avait reçu son indemnité du gouvernement canadien, mais pas celle du gouvernement britannique, qui aurait dû lui parvenir en même temps. Quand il avait demandé le solde au ministère de la Défense nationale, celui-ci avait refusé, en se fondant semble-t-il sur la lettre de l'Amirauté britannique comme preuve que la somme avait déjà été payée.

L'ancien combattant a poursuivi ses démarches sans désespérer, avec l'aide de plusieurs députés fédéraux et de plusieurs ministres de la Défense. Sa demande a été rejetée chaque fois, parce que le Ministère revenait toujours aux lettres les plus récentes pour prouver qu'il avait tort de réclamer. Pourtant, personne n'avait jamais vérifié les originaux pour voir où l'erreur s'était produite.

En désespoir de cause, le plaignant a invoqué la Loi, espérant par là passer outre à toutes les lettres faisant suite aux originaux contenus dans son relevé de paye, pour pouvoir examiner les originaux eux-mêmes. Il a porté plainte au Commissaire quand il a constaté qu'aucun des documents qu'on lui avait communiqués ne prouvait qu'on lui avait payé la somme en question. Il a prétendu que les documents qu'il cherchait devaient avoir été retenus.

L'enquête n'a rien révélé de nouveau; le plaignant avait reçu tous les documents figurant au dossier. Il semblait, d'après un vieux document de paye, que le paiement de l'Amirauté britannique avait été porté à son compte. La somme en litige avait alors été considérée comme payée, sur la foi de la lettre de l'Amirauté, et elle avait été déduite du montant dû.

Le Commissaire a conclu que le Ministère n'avait refusé l'accès à aucun document. Il n'y avait pas de preuve documentaire que le paiement avait été fait. Le Commissaire a communiqué ses constatations au plaignant par écrit, en lui suggérant de montrer la lettre au ministre de la Défense, car son contenu aurait pu contribuer à régler une affaire qui traînait depuis 40 ans.

Quand le Commissariat a essayé de faire un suivi en communiquant avec le plaignant, celui-ci avait déménagé sans laisser d'adresse.

Retourner son courrier a révélé qu'il était un détenu

Un détenu a porté plainte au Commissaire en disant que le personnel du pénitencier de Kingston avait retourné deux de ses colis aux expéditeurs, en leur disant qu'il n'était pas autorisé à les recevoir, puisqu'il était détenu dans un pénitencier. Le plaignant a allégué qu'on avait porté atteinte à sa vie privée sans justification en révélant qu'il était un détenu.

Les deux colis, dont l'un venait du Sénat des États-Unis et l'autre du Service du tourisme du gouvernement manitobain, contenaient des cartes routières et de la documentation touristique. Les détenus ne sont pas autorisés à avoir des cartes routières et des brochures décrivant la région du pénitencier, parce qu'il pourraient s'en servir pour préparer une évasion. Le détenu avait auparavant eu droit à d'autre matériel touristique.

Le Service correctionnel du Canada (SCC) a déclaré à l'enquêteur que les détenus ne sont pas autorisés à recevoir des postes de radio, des livres, etc. Le personnel ouvre tous les colis et les fouille pour vérifier s'ils contiennent des articles interdits, auquel cas ils sont refermés et renvoyés à l'expéditeur avec une note invoquant la disposition pertinente des ordres permanents du pénitencier. Le SCC a maintenu que le fait que quelqu'un est détenu dans un pénitencier est du domaine public.

Le Commissaire a fait remarquer au SCC que son propre code de communication des renseignements ne l'autorise pas à révéler le lieu où les détenus sont incarcérés, pour éviter de nuire à leur éventuelle réinsertion sociale.

Parallèlement, le détenu avait présenté un grief interne sur plusieurs questions, dont celle de la communication de son statut. Quand on a fait droit à son grief, au deuxième palier, le pénitencier a cessé de déclarer aux expéditeurs que les récipiendaires des colis retournés étaient des détenus.

Le Commissaire a recommandé au SCC de se donner une politique pour faire en sorte qu'un incident comme celui-ci ne se répète pas. Au début de la présente année, le SCC a distribué dans tous ses établissements régionaux une politique en vertu de laquelle le courrier doit être retourné «avec discernement».

La nouvelle politique précise qu'il suffit d'indiquer sur les lettres ou les colis retournés qu'ils sont refusés, en les renvoyant à l'expéditeur sans autre forme d'explication.

Le Commissaire a jugé la plainte bien fondée et résolue.

Le plaignant a eu accès aux documents du comité d'examen

Un homme s'est plaint au Commissaire que la Société canadienne des postes lui avait refusé l'accès aux représentations faites à un comité d'examen et au rapport final de ce comité.

Le plaignant voulait voir tous les documents étudiés par le comité pour déterminer si la Société avait eu suffisamment de preuves qu'il distribuait de la propagande haineuse pour justifier l'interception de son courrier.

La Société a rétabli son service après avoir reçu le rapport du comité, qui avait tenu des audiences publiques.

Le plaignant a aussi prétendu que la Société avait communiqué à un tiers le rapport qu'elle lui avait refusé et que ce tiers en avait cité des extraits au cours d'une entrevue accordée à un journal.

L'enquêteur du Commissariat a commencé par constater que la Société n'avait pas examiné les documents page par page avant de décider qu'elle pourrait refuser, pour divers motifs, la communication des dix volumes du dossier en question. A la demande de l'enquêteur, le personnel de la Société a étudié le dossier et invoqué des exceptions pour les motifs suivants :

*renseignements personnels obtenus à titre confidentiel d'un autre gouvernement, article 19;

*renseignements obtenus ou préparés par un organisme d'enquête, alinéa 22(1)(a);

*renseignements dont la divulgation risquerait de nuire à la sécurité des individus, article 25;

*renseignements concernant d'autres individus, article 26;

*renseignements protégés par le secret professionnel liant un avocat à son client, article 27.

Les Services de sécurité et d'enquête de la Société constituent un organisme d'enquête aux fins de la *Loi sur la protection des renseignements personnels*. Par conséquent, la Société pouvait refuser de communiquer la plus grande partie des renseignements demandés. Toutefois, l'accès au rapport du comité ne pouvait être refusé pour cette raison, pas plus d'ailleurs que les documents présentés aux audiences du comité par l'Association canadienne des libertés civiles et par un témoin expert.

La Société a consenti à réétudier ces documents, et elle a cessé de soutenir que la communication de certains des renseignements risquait de nuire à la sécurité d'autres individus.

Après des mois de négociations, la Société a autorisé le plaignant à étudier le rapport du comité et la transcription des dires du témoin expert. Comme elle continuait néanmoins à refuser de lui communiquer le texte des représentations de l'Association, l'enquêteur du Commissariat a proposé à la Société de demander à l'Association de l'autoriser à les communiquer. L'Association y a consenti et la Société a mis les documents à la dispositions du plaignant.

Le Commissaire a conclu que les autres exceptions étaient appropriées, et il a jugé la plainte bien fondée et résolue.

Par ailleurs, le Commissariat n'a pas pu faire enquête sur l'allégation du plaignant à l'effet que le rapport avait été communiqué illégalement, parce que cela s'était produit avant l'entrée en vigueur de la Loi.

On avait dit à la police que le détenu aurait accès aux rapports

La Loi interdit la communication des renseignements fournis «à titre confidentiel» par d'autres gouvernements. Le résultat des enquêtes sur les cas de refus de communiquer ce genre de renseignements est souvent prédictible, car ils ne peuvent être divulgués s'ils ont été désignés confidentiels par un gouvernement provincial ou par des autorités municipales.

Pourtant, l'enquêteur du Commissariat a constaté dans deux cas que la Commission nationale des libérations conditionnelles (CNLC) et le Service correctionnel du Canada (SCC) avaient tous deux refusé de communiquer ces renseignements à un détenu, même si l'agent des libérations conditionnelles avait déclaré au corps de police municipal d'où les renseignements provenaient que le détenu aurait accès aux renseignements, et que le corps de police y avait consenti.

L'enquêteur a constaté que d'autres renseignements fournis à titre confidentiel par le gouvernement provincial n'avaient pas non plus été communiqués. Le Commissaire a conclu que le refus de communiquer ces derniers renseignements était justifié, contrairement à celui de refuser l'accès aux renseignements fournis par le corps de police.

La CNLC et le SCC ont consenti à la communication des renseignements provenant du corps de police.

Il y avait des données fiscales dans le dossier de harcèlement.

La Loi précise que des renseignements recueillis à une fin ne peuvent pas être utilisés à une autre, à moins que la seconde soit compatible avec la première.

C'est pour cette raison qu'un fonctionnaire de Revenu Canada (Impôt) a porté plainte au Commissaire, alléguant que le Ministère s'était servi de ses renseignements fiscaux dans une enquête sur un cas de harcèlement.

Le plaignant faisait l'objet d'une enquête disciplinaire quand il s'est plaint d'avoir été injustement choisi pour faire l'objet d'une vérification fiscale. L'enquêteur du Commissariat a étudié le dossier de l'enquête sur le harcèlement et il y a trouvé plusieurs allusions à la situation fiscale du plaignant. Il a aussi trouvé la preuve que l'enquêteur sur le harcèlement avait eu accès à la déclaration d'impôt du plaignant.

Le Commissaire a jugé que les données fiscales n'auraient pas dû être versées dans le dossier de harcèlement, et que l'enquêteur du Ministère n'aurait pas dû non plus avoir accès à la déclaration de revenu.

Quand le Commissaire a déclaré à Revenu Canada que la plainte était bien fondée, celui-ci lui a demandé de tenir compte de faits nouveaux. Le Commissaire a accepté de le faire, mais les entrevues subséquentes ne lui ont rien appris de plus. Même s'il y avait des données fiscales confidentielles dans les dossiers personnels du plaignant, la direction du Ministère a persisté à dire qu'elle lui avait imposé une sanction disciplinaire en raison des conclusions de l'enquête sur le harcèlement, et non à cause des données fiscales.

Le Commissaire n'a pas pu conclure que les données fiscales avaient été utilisées à des fins disciplinaires, car leur seule présence dans des dossiers bien distincts constituait une infraction aux termes de la Loi. Il a répété que la plainte était bien fondée.

Pas question de demander des détails à un autre employeur

Un travailleur de la Nouvelle-Écosse s'est plaint que la Société canadienne des postes avait obtenu et communiqué des renseignements personnels le concernant pour régler sa réclamation d'indemnité d'accident du travail. Le plaignant était allé travailler à la Société pendant une grève postale, à un moment où il était en congé d'un autre emploi; il avait été blessé au cours de son premier quart de travail et il avait réclamé une indemnité.

Les employeurs doivent étayer les demandes d'indemnité d'accidents du travail de leurs employés en décrivant les tâches que ceux-ci doivent normalement exécuter à leur retour au travail, ainsi qu'en produisant un rapport médical sur leur aptitude à exécuter ces tâches à ce moment-là. Comme le plaignant n'était pas l'un de ses employés permanents, la Société a obtenu les renseignements nécessaires de son autre employeur et d'un médecin qu'elle avait choisi. Elle a envoyé ces renseignements à la Commission des accidents du travail de la Nouvelle-Écosse, qui devait se charger du reste.

L'enquête du Commissariat avait pour but de déterminer si la *Loi sur les accidents du travail* de la province obligeait la Société à recueillir et communiquer les renseignements en question. À cette fin, le Commissaire a demandé à la Commission provinciale de lui préciser les renseignements que les employeurs sont tenus de lui fournir pour étayer les demandes d'indemnité.

Après avoir reçu la réponse de la Commission, le Commissaire a conclu que la Société avait le droit de recueillir des renseignements sur les circonstances de l'accident survenu dans ses locaux, mais qu'elle n'avait ni le droit, ni le devoir d'en obtenir de l'autre employeur du plaignant. En outre, la Commission n'avait pas demandé à la Société de détails sur l'aptitude du plaignant à reprendre son travail, du point de vue médical. Il semble que la Société n'ait jamais informé le plaignant de l'identité des autres parties à qui elle pourrait fournir le rapport médical pertinent.

Le Commissaire a conclu que la plainte était bien fondée. La Société a depuis adopté de nouvelles procédures régissant la préparation des demandes d'indemnité du travail des gens blessés dans ses locaux mais travaillant essentiellement ailleurs.

On ne justifie pas un congédiement en se fondant sur une demande d'indemnité d'accident du travail

Une fonctionnaire s'est plainte au Commissaire que le Service correctionnel du Canada (SCC) lui avait ordonné de subir des tests psychologiques à l'appui de sa demande d'indemnité d'accident du travail, puis s'était servi des rapports médicaux pour la congédier.

La plaignante, qui était agente de gestion de cas dans un pénitencier fédéral, a reçu l'ordre de subir les tests pour étayer sa demande d'indemnité en raison du stress que lui causait le harcèlement sexuel des détenus à son endroit.

L'enquête a confirmé que les tests avaient bien eu lieu pour étayer la demande d'indemnité et qu'on n'avait pas dit à la plaignante que les résultats pourraient servir à justifier son renvoi. (En fait, le SCC a aussi utilisé les résultats des tests pour rejeter sa candidature à un autre poste.)

Le Commissaire a conclu que le SCC s'était servi des résultats des tests à mauvais escient, et que la plainte était bien fondée. IL a demandé au SCC de garantir que la situation ne se répéterait pas. Depuis, le SCC a distribué un code de protection de la vie privée de ses fonctionnaires à tous ses employés.

La communication des renseignements médicaux n'est pas indispensable

Plusieurs fonctionnaires affectés à la région Huron de la Société canadienne des postes se sont plaints au Commissaire que la Société menaçait de mesures disciplinaires tous ceux qui refuseraient de remplir «volontairement» une formule de consentement à ce que leur médecin communique à la Société des renseignements médicaux les concernant.

L'enquête a révélé que, dans chaque cas, le fonctionnaire intéressé avait pris des congés de maladie et qu'il avait rempli la formule requise d'évaluation d'aptitude à travailler à son retour au travail. La direction locale de la Société jugeait qu'elle n'avait pas assez de renseignements, car la formule ne comporte pas de diagnostic; elle avait demandé aux intéressés de consentir à ce que leur médecin lui donne les renseignements médicaux qu'elle jugeait avoir besoin.

Les fonctionnaires qui ont refusé de signer la formule de consentement ont subi des mesures disciplinaires pour «insubordination» et ils ont été avertis que, s'ils persistaient dans leur refus, ils pourraient être renvoyés.

Quand l'administration centrale de la Société a été saisie des plaintes, elle a ordonné qu'on mette immédiatement fin à la pratique contestée, et le directeur régional des relations du travail a annulé les renvois qu'on lui avait signalés. Toutefois, en dépit des mesures promises, les plaintes ont été maintenues. Il semble y avoir eu rupture de communication.

En fin de compte, l'administration centrale de la Société a informé tous ses directeurs généraux régionaux qu'ils n'avaient pas le droit d'obtenir des renseignements médicaux détaillés et délicats, et que les fonctionnaires qui signent une formule de consentement à la communication de renseignements de ce genre doivent le faire en toute liberté. La Société a accepté d'annuler toutes les mesures disciplinaires prises contre les intéressés et de les dédommager pour toutes les pertes subies par suite des suspensions.

Les associés ont tous le droit d'avoir les renseignements qui les concernent

Plusieurs plaintes logées contre Revenu Canada (Impôt) ont amené le Commissariat à se pencher sur les dispositions juridiques complexes qui régissent le droit d'accès d'associés dans une société en commandite aux renseignements fiscaux qui les concernent tous.

Les associés en question voulaient interjeter appel de leur avis de cotisation après que Revenu Canada eut refusé d'accepter les pertes et les crédits d'impôt à l'investissement que leur société avait réclamés en 1985. Ils ont donc demandé qu'on leur communique des renseignements concernant notamment des détails sur les négociations conduites entre l'associé directeur général et le fisc.

Revenu Canada a prétendu que la communication des renseignements demandés nuirait à l'application de la *Loi de l'impôt sur le revenu*. Il a aussi invoqué les dispositions restrictives de l'article 241 de cette Loi sur le caractère confidentiel des renseignements fiscaux, qui interdisent la communication de ces renseignements à quiconque, sauf aux contribuables intéressés. Le Ministère estimait que ces dispositions (qui rendent ses fonctionnaires criminellement responsables de tout manquement à la règle de la confidentialité) prévalaient sur le droit d'accès reconnu par la *Loi sur la protection des renseignements personnels*.

En fait, les plaignants ont reçu plus de renseignements après la modification de *Loi de l'impôt sur le revenu* de 1988, qui a précisé les renseignements qu'un particulier peut recevoir afin d'interjeter appel d'une décision fiscale. Néanmoins, les nouveaux renseignements communiqués aux plaignants ne contenaient rien qui leur avait été refusé en vertu de la *Loi sur la protection des renseignements personnels*.

La société en cause avait été créée en vertu de la *Loi sur les sociétés en nom collectif* du Manitoba, qui dispose que les associés peuvent «consulter les livres de la firme, étudier l'état ainsi que les progrès de l'entreprise de la société en commandite.» En outre, les associés dans une société en commandite ont une relation individuelle avec le fisc, et ils sont individuellement tenus de payer leurs impôts. Les renseignements que les associés réclamaient étaient personnels, en ce qu'ils les touchaient individuellement, mais ils étaient aussi collectifs, étant donné qu'ils les concernaient tous.

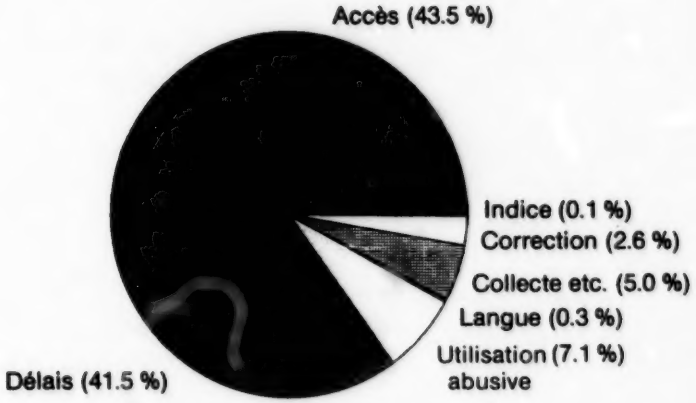
Le Ministère a déclaré que, puisque les renseignements concernaient chacun des associés, il lui était impossible de les communiquer à l'un d'entre eux sans le consentement de tous les autres. Le Commissaire a maintenu pour sa part que, puisque les renseignements étaient personnels et concernaient chacun des plaignants, le Ministère ne pouvait refuser de les communiquer simplement parce qu'ils étaient identiques aux renseignements sur tous les autres associés. À son avis agir de la sorte aurait tout simplement nié le droit d'accès reconnu à chacun des associés par la *Loi sur la protection des renseignements personnels.* Il a aussi demandé au Ministère de prouver comment le fait de donner aux associés l'accès qu'ils réclamaient à ces renseignements personnels aurait porté atteinte à la *Loi de l'impôt sur le revenu.*

Le Commissaire s'est dit d'accord sur un certain nombre d'exceptions invoquées par le Ministère pour refuser de communiquer les renseignements personnels concernant seulement tel ou tel associé, les renseignements fournis à titre confidentiel par une province et enfin les renseignements échangés entre le Ministère et ses avocats (qui sont protégés par le secret professionnel).

Après de longues semaines de discussions, le Ministère a reconnu qu'il ne pouvait faire la preuve d'aucune atteinte à la *Loi de l'impôt sur le revenu.* Il a aussi reconnu que les renseignements personnels concernant tous les associés devraient être mis à la disposition de chacun d'entre eux.

Revenu Canada a donc communiqué plus de 2 000 pages de renseignements aux plaignants.

Plaintes réglées par motifs 1989-90

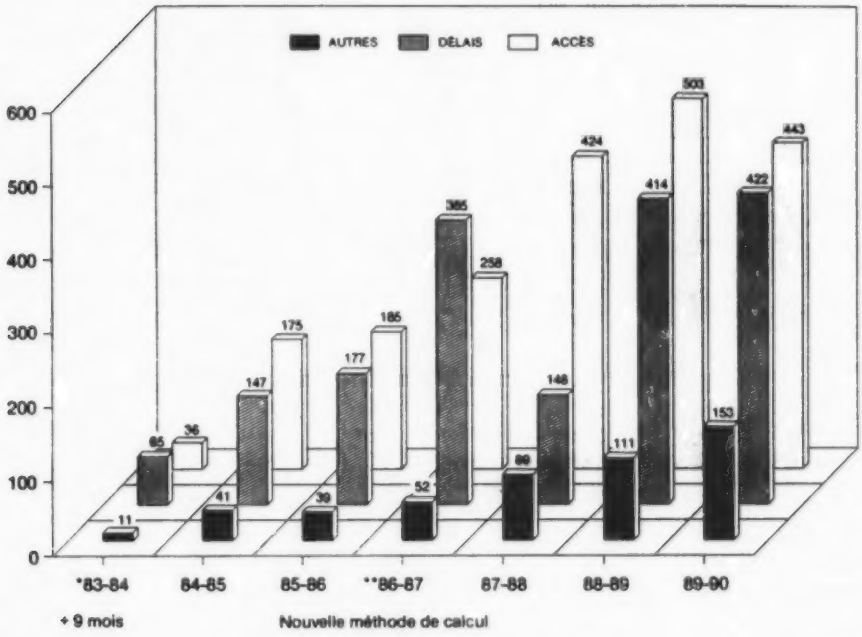


Plaintes réglées par institution et résultats

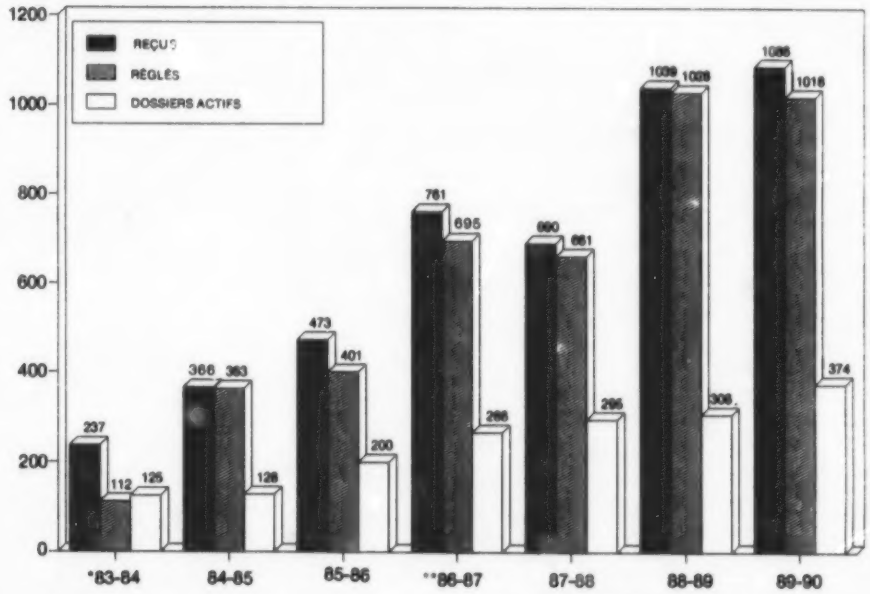
Ministère	Nombre	Bien fondée	Bien fondée résolue	Non fondée	Abandonnée
Affaires des anciens combattants Canada	5	0	1	4	0
Affaires extérieures Canada	5	1	0	4	0
Affaires indiennes et du Nord Canada	10	0	0	10	0
Agriculture Canada	1	0	0	1	0
Approvisionnements et services Canada	1	0	0	1	0
Archives nationales Canada	8	0	1	7	0
Bureau canadien de la sécurité aérienne	1	0	1	0	0
Bureau de l'enquêteur correctionnel	1	1	0	0	0
Bureau du Conseil privé	1	0	0	1	0
Commissariat aux langues officielles	5	0	2	1	2
Commission canadienne droits de la personne	1	0	0	1	0
Commission de la Capitale nationale	1	1	0	0	0
Commission de la Fonction publique	15	1	4	9	1
Commission des relations de travail dans la Fonction publique	1	0	0	1	0
Commission nationale des libérations conditionnelles	29	5	13	11	0
Communications, Ministères des	3	0	2	1	0
Conseil de la radiodiffusion et des télécommun. canadiennes	43	1	0	42	0

Ministère	Nombre	Bien fondée	Bien fondée résolue	Non fondée	Abandonnée
Conseil de recherches médicales	1	0	0	1	0
Défense nationale	117	74	14	25	4
Emploi et immigration Canada	53	13	18	17	5
Gendarmerie royale du Canada	47	4	6	35	2
Justice Canada, Ministère de la	7	1	3	3	0
Monnaie royale canadienne	1	1	0	0	0
Revenu Canada - Douanes et Accise	7	2	3	2	0
Revenu Canada - Impôt	59	38	11	7	3
Santé et Bien-être social Canada	67	25	16	23	3
Secrétariat d'Etat	2	0	0	2	0
Service canadien du renseignement de sécurité	38	2	4	32	0
Service correctionnel Canada	395	188	59	122	26
Société canadienne d'hypothèque et de logement	1	0	1	0	0
Société canadienne des postes	61	21	9	30	1
Société du crédit agricole Canada	1	0	1	0	0
Solliciteur général Canada	15	0	1	14	0
Transports Canada	7	4	2	0	1
Travail Canada	5	0	1	3	1
Travaux publics Canada	3	1	2	0	0
TOTAL	**1018**	**384**	**175**	**410**	**49**

Plaintes réglées et motifs 1983-1990



Nombre de dossiers 1983-1990



+ 9 mois

* Nouvelle méthode de calcul

Demandes générales d'informations

Une fois de plus, le nombre de demandes générales d'informations adressées au Commissariat s'est accru de façon substantielle, passant de 2041 qu'il était l'an dernier à 3447 cette année. Or, cette augmentation reflète un accroissement réel de la charge de travail et ne résulte donc pas seulement d'une meilleure méthode de comptabilisation des demandes, comme c'était le cas en 1988-1989. Cette augmentation va obliger le Commissariat à embaucher un autre agent pour répondre aux appels et au courrier.

La proportion des demandes d'interprétation de la Loi a augmenté : elle représente 59 p. 100 du total, par rapport à 46 p. 100 l'an dernier. Les gens n'aiment pas que leur employeur leur demande des renseignements médicaux ou des documents d'identité tels que des certificats de mariage ou de naissance. Quelqu'un a même téléphoné pour demander quoi faire après s'être fait réclamer une liste complète de ses dépenses personnelles. Les demandes de renseignements de ce type donnent parfois lieu à des plaintes.

Les représentants des syndicats de la Fonction publique ont souvent téléphoné au Commissariat pour demander des renseignements sur diverses questions. Par exemple, le syndicat peut-il exiger un relevé des salaires exacts de ses membres plutôt que les échelles de traitement, qui sont du domaine public aux termes de la Loi? (En l'occurrence, le syndicat voulait obtenir confirmation que l'employeur lui versait la cotisation voulue). Le Commissariat a suggéré au syndicat de retenir les services d'un vérificateur indépendant pour confirmer l'exactitude de ces renseignements, au lieu de chercher à en obtenir la communication.

Des députés fédéraux téléphonent et écrivent au Commissariat au sujet des préoccupations de leurs commettants, qui tiennent à protéger leur vie privée. Ainsi, un électeur s'inquiétait des sondages téléphoniques de Statistique Canada. Il avait écrit pour se plaindre d'avoir à répondre à des questions personnelles au téléphone, étant donné qu'il ne pouvait pas confirmer l'identité de la personne qui l'appelait. Le fait est que Statistique Canada a de plus en plus recours aux sondages téléphoniques. Toutefois, les répondants en sont habituellement informés à l'avance par lettre ou par téléphone, et Statistique Canada leur fournit un numéro à composer pour confirmer l'identité de l'enquêteur.

Les demandes d'informations portant sur le numéro d'assurance sociale (NAS) ont légèrement diminué à 19 p. 100, comparativement à 21 p. 100 l'an dernier. Plusieurs se sont dits mécontents d'être obligés de communiquer leur NAS en raison des modifications apportées à la *Loi de l'impôt sur le revenu*. Une dame, qui avait été autorisée à ne pas utiliser son NAS pour des motifs d'ordre religieux, a demandé l'aide du Commissariat parce que les modifications apportées à la Loi signifiaient qu'elle pouvait être pénalisée si elle refusait de divulguer son NAS. Le Commissariat a découvert que, contrairement aux Américains, les Canadiens ne peuvent être relevés de l'obligation d'avoir un NAS, même pour des motifs d'ordre religieux.

Les demandes de renseignements sur les organisations qui ne sont pas assujetties à la Loi sont passées à 16 p. 100, comparativement à 15 p. 100 l'an dernier. De ces demandes, 4 p. 100 portaient sur des institutions fédérales échappant à la Loi et 12 p. 100 sur des organisations ne relevant pas du gouvernement fédéral. Par exemple, une fonctionnaire ontarienne voulait savoir si l'organisme où elle travaillait pouvait demander à ses employées si elles avaient l'intention d'être enceintes au cours de l'année budgétaire à venir. Le Commissaire l'a renvoyée à son homologue ontarien. (L'institution fédérale qui poserait une question comme celle-là contreviendrait à la Loi fédérale.)

Le nombre de demandes adressées au Commissariat par erreur est demeuré stable, soit 7 p. 100 comparativement à 8 p. 100 l'an dernier. Le Commissariat a fait suivre ces demandes au ministère ou à l'organisme intéressé.En outre, 6 p. 100 des demandes n'avaient rien à voir avec le mandat du Commissaire; dans la mesure du possible, elles ont été soumises à qui de droit.

Le central téléphonique du Commissariat (partagé avec le Commissariat à l'information) a renvoyé 8254 appels aux bureaux de Référence Canada dans tous les coins du pays.

Les deux Commissariats ont fait modifier leurs inscriptions dans les pages bleues des bottins téléphoniques, pour mieux expliquer leur mandat. Toutefois, la combinaison du mot «information» dans le titre avec une ligne nationale sans frais leur attire de nombreux appels téléphoniques qui n'ont rien à voir avec leur mission… et qui coûtent cher.

Direction générale de l'observation

Rétrospective sur les sept dernières années

Depuis l'entrée en vigueur de la Loi, le 1er juillet 1983, le Commissariat a fait des vérifications dans 27 institutions gouvernementales, pour déterminer dans quelle mesure elles respectaient la Loi. De plus, il a fait une vérification dans 11 institutions pour déterminer si leurs fichiers de renseignements personnels pouvaient vraiment être considérés comme inconsultables, et il a enquêté sur plus de 16 cas de pertes ou de vols de renseignements personnels.

Pour faire respecter la Loi, le Commissariat a dû innover, en faisant appel à un nouveau genre de spécialiste, le «vérificateur de la protection de la vie privée», à la fois enquêteur, vérificateur, gestionnaire de dossiers et spécialiste du TED.

La vérification est une activité à la fois ancienne et nouvelle. L'essentiel des tâches qu'elle implique date du début du siècle, mais les techniques ont évolué au fil des vérifications opérationnelles, de celles qui sont fondées sur les systèmes, des évaluations de rapport qualité-prix et enfin de la vérification intégrée, omniprésente de nos jours.

Pourtant, il est impossible de savoir si les méthodes de traitement de l'information d'une institution quelconque sont conformes à la Loi, si l'on n'utilise pour ce faire que les techniques consacrées de la vérification classique, dont la méthode et les instruments ont presque exclusivement pour but de déterminer le volume et la valeur financière des activités plutôt que d'établir si elles satisfont à un certain nombre de critères.

Depuis l'entrée en vigueur de la Loi, le Commissariat a mis au point des instruments et des méthodes de vérification d'énormes fichiers de renseignements personnels, afin d'assurer le déploiement optimal de ses maigres ressources de vérification. Il s'est donné les moyens d'étudier et d'évaluer la relation complexe entre les articles 7 et 8 de la Loi, en ce qui concerne la sécurité des systèmes d'information.

Le vérificateur moyen d'aujourd'hui se sert de techniques et d'instruments d'échantillonnage calibrés en dollars, alors que le vérificateur de l'observation ne dispose que de questionnaires maison, d'une approximation pour établir son échantillon de dossiers et d'un guide de haut niveau pour voir dans quelle mesure les institutions respectent la Loi.

La première étape de la vérification, en matière de protection de la vie privée, consiste à déterminer si les renseignements personnels :

*sont recueillis seulement lorsque leur collecte est autorisée aux fins d'une activité ou d'un programme donné;

*sont conservés juste le temps qu'il faut pour être utilisés à leur fin originale, mais assez longtemps pour que les personnes concernées aient un délai raisonnable pour y avoir accès;

*sont utilisés seulement aux fins pour lesquelles ils ont été recueillis, ou à des fins compatibles avec elles;

*ne sont communiqués à des tiers que quand leur communication est autorisée par la Loi sur la protection des renseignements personnels;

*sont retirés à la fin de leur période d'utilité, conformément aux normes des Archives nationales;

*sont protégés, conformément à la politique du gouvernement sur la sécurité.

Les vérifications de la Direction de l'observation de la Loi ont pour objet de déterminer si les institutions assujetties à la Loi ont satisfait à ces six critères dans la gestion des renseignements personnels contenus dans leurs systèmes. Pour ce faire, il faut avoir recours à un instrument permettant d'établir un échantillon statistiquement suffisant de fichiers de renseignements personnels pouvant contenir de quelques douzaines à plusieurs millions de dossiers, puis identifier les dossiers particuliers à vérifier. Le premier programme automatisé du genre a été conçu, mis à l'essai et mis au point par le Commissariat, qui s'en sert dans toutes ses vérifications. C'est l'un des éléments fondamentaux de la méthode utilisée par les institutions qui font leurs propres vérifications de l'observation de la Loi. Il a été utilisé avec succès pour la vérification de tous les types de fichiers, des plus petits, dans lesquels les renseignements sont consignés à la main, aux bases de données interconnectées et automatisées les plus massives.

La deuxième étape de la vérification a consisté à élaborer une matrice analytique automatisée comprenant les critères propres à déterminer les risques relatifs pour toutes les institutions assujetties à la Loi. À partir de données obtenues grâce à un questionnaire distribué en 1986 à toutes ces institutions, le Commissariat a obtenu un modèle informatique dont il s'est servi pour lancer des projets de vérification en se fondant sur des critères mesurables plutôt que sur des hypothèses, si valables soient-elles. Les données de mise à jour sont collectées une fois l'an, de façon que le modèle puisse être adapté à la situation.

La troisième étape a été la mise au point d'une méthode de travail appropriée, avec la documentation nécessaire, de façon que les nouveaux arrivants au Commissariat puissent profiter des leçons de l'expérience et que les activités de vérification, les rapports et les documents de travail soient conséquents. L'élaboration de la méthode a commencé presque au tout début de la vérification et elle se poursuit encore.

Enfin, la quatrième étape a été l'intégration des expériences acquises et des instruments mis au point pour la vérification de la dernière génération des systèmes de traitement de l'information, ainsi que l'examen et l'évaluation des implications de la technologie nouvelle pour la sécurité, dans la mesure où cette technologie touche les renseignements personnels.

C'est une lourde tâche, mais le Commissariat a remporté certains succès. Il a réussi à établir de nouvelles relations avec les organismes responsables de l'élaboration des politiques et de leur application, comme le Conseil du Trésor, le Centre de sécurité des télécommunications et la GRC, qui disposent de spécialistes en politiques et en technologie de l'information. En outre, le Commissariat trouve sans cesse des homologues dans les administrations provinciales, dans l'entreprise privée et dans les associations de spécialistes intéressés, comme l'Association canadienne de l'informatique, la Information Systems Security Association et l'Institut des vérificateurs internes.

Au cours de la première année d'application de la nouvelle méthode et des nouveaux instruments de vérification, le Commissariat s'est penché sur quatre grands ministères. L'année suivante, il a réalisé six vérifications complètes. Cette année, il en a conclu 14, en plus de faire enquête sur cinq incidents. Au cours des années à venir, il concentrera ses efforts dans les plus importantes des institutions, qui détiennent les renseignements personnels les plus délicats dans les systèmes d'ordinateur les plus perfectionnés. La principale leçon à tirer de l'expérience de vérification du Commissaire, c'est que la vérification ne consiste pas du tout à prendre les gens en faute. C'est plutôt une collaboration qui fera de l'observation de la Loi une réalité.

Si les intéressés ne partagent pas leurs expériences et leurs connaissances et s'ils ne participent pas à des vérifications conjointes, chercher à assurer l'observation de la Loi ne sera jamais qu'un cauchemar pour les responsables. La Loi ne sera vraiment bien respectée que lorsque toutes les institutions, fédérales, provinciales ou privées, reconnaîtront la nécessité d'un ensemble de pratiques équitables de gestion des renseignements personnels et qu'elles seront conscientes de leurs avantages.

Pendant l'année la direction de l'observations a fait des vérifications dans les institutions suivantes : Approvisionnements et Services Canada, Centre de recherches pour le développement international, Commission canadienne d'examen des exportations de biens culturels, Commission des relations de travail dans la Fonction publique, Comité de surveillance des activités de renseignements de sécurité, Commission de réforme du droit du Canada, Conseil de recherches en sciences humaines du Canada, Santé et Bien-être social du Canada (Services médicaux, Programmes de la sécurité du revenu et la Direction générale de l'administration du personnel), Société canadienne des brevets et d'exploitation Ltée et la Société pour l'expansion des exportations.

Constatations

Les vérifications réalisées dans les ministères ont globalement révélé les mêmes faiblesses que celles que le Commissaire a signalées dans ses rapports antérieurs. Il est donc évident que le manque de sensibilisation à la Loi continue d'être extrêmement préoccupant. Les fonctionnaires fédéraux ignorent souvent quels sont leurs droits en rapport avec la vie privée (ou ceux de leurs clients) et ils ne connaissent pas les exigences de la Loi en regard de la façon dont ils traitent quotidiennement les renseignements personnels avec lesquels ils travaillent. Par conséquent, ils risquent de mal protéger et de communiquer indûment les données personnelles concernant leurs clients. Si l'on consacrait plus de ressources à la formation en matière de protection de la vie privée, on contribuerait à éliminer ce risque.

Les vérificateurs ont par ailleurs constaté que les cueillettes de renseignements personnels sont souvent décrites incorrectement (ou seulement partiellement) dans le *Répertoire des renseignements personnels*, de sorte qu'il est difficile - voire impossible - pour les gens qui désirent demander qu'on leur communique des renseignements de savoir s'ils existent. Il arrive que les renseignements personnels ne soient pas groupés par cueillette et, par conséquent, qu'ils ne soient pas structurés de façon suffisamment systématique pour qu'il soit possible de tenter de les décrire.

Plusieurs des institutions qui ont fait l'objet d'une vérification cette année ne respectaient pas les délais établis par les Archives nationales pour la conservation et le retrait des renseignements personnels. Par conséquent, elles risquent d'utiliser trop longtemps des renseignements incorrects ou de ne pas avoir de renseignements à jour, lorsqu'elles les retirent trop tôt et ce, sans compter qu'une telle accumulation inutile de documents peut encombrer leurs salles de dossiers (mais ce dernier aspect n'a rien à voir avec la Loi).

Souvent, les superviseurs ou d'autres employés ont accès à des dossiers du personnel même s'ils n'ont pas besoin de savoir ce qu'un fonctionnaire donne à des oeuvres de charité, quelle est sa situation familiale ou son état de santé, s'il achète des obligations d'épargne ou s'il est réputé ne pas être en situation de conflit d'intérêts.

L'insuffisance des mesures de protection des renseignements personnels revient souvent sur le tapis. Le gouvernement a consacré une grande partie de ses ressources et de son attention à la mise en place de mesures propres à assurer une protection appropriée des renseignements considérés comme d'intérêt national (confidentiels, secrets et très secrets). Pourtant, les conséquences résultant de la perte de renseignements personnels ou de leur accès par des personnes non autorisées peuvent s'avérer catastrophiques pour l'individu concerné, sans pour autant nuire à l'intérêt national. L'utilisation des télécopieurs en est un excellent exemple. Alors qu'on applique régulièrement des normes de codage bien établies pour transmettre des renseignements protégés d'intérêt national, on communique tous les jours des renseignements personnels pourtant délicats sans songer le moindrement à les protéger.

Les ministères peuvent bien juger vétilleuses et coûteuses les recommandations du Commissaire, mais s'il les fait, c'est parce qu'il prend vraiment au sérieux le risque que la transmission par télécopieur présente pour les renseignements personnels.

D'autre part, le Commissariat constate régulièrement des manquements à la sécurité qui peuvent sembler mineurs, mais qui pourraient néanmoins se révéler désastreux. Par exemple, les codes d'accès d'ordinateur inchangés restent affichés sur les terminaux, les clés de classeurs traînent dans des tiroirs non verrouillés, les serrures n'offrent pas toujours une protection suffisante, les préposés au nettoyage peuvent circuler sans surveillance, les registres de ceux

qui ont accès aux dossiers sont incomplets, des documents contenant des renseignements souvent très délicats sont tout simplement jetés à la poubelle, et ainsi de suite. En fait, certaines des précautions les plus élémentaires que nous prenons pour protéger nos biens à la maison semblent totalement négligées, dans l'administration fédérale, lorsqu'il s'agit des renseignements personnels.

Aucune institution fédérale, même pas le Commissariat lui-même, n'a une fiche vierge en matière de la protection de la vie privée. Et aucune institution ne peut se permettre d'attendre la visite des vérificateurs de la vie privée pour agir.

Et pourtant, tout n'est pas si noir, car il y a plusiers aspects positifs à signaler. Les ministères se sont montrés très sensibles à la Loi et ils désirent vraiment la respecter. Le Commissariat n'a jamais découvert d'infractions systématiques ou délibérées à la Loi. Les contrevenants corrigent rapidement leurs erreurs et leurs lacunes, sans se faire tirer l'oreille. De plus en plus de ministères ont fait de l'observation de la Loi une partie intégrante de leurs vérifications internes régulières. Bien sûr, après avoir fait des vérifications dans 27 institutions seulement sur 150, le Commissariat n'a peut-être pas un échantillon suffisamment représentatif pour généraliser, mais il se doit de reconnaître les réalisations importantes. Cela dit, personne ne devrait s'asseoir sur ses lauriers, car les vérifications continuent.

QUELQUES ENQUÊTES SUR DES INCIDENTS

Les rapports d'enquête sur les accidents sont protégés

Le Commissariat a voulu en savoir plus long après qu'un journaliste eut prétendu que la Société d'assurances publiques du Manitoba s'était servie d'un rapport d'accident de Transports Canada pour refuser de dédommager une victime d'un accident de la route.

Le journaliste du *Winnipeg Free Press* avait décrit comment la Société avait refusé la demande de la victime parce qu'un rapport de Transports Canada, qui lui imputait une partie de la responsabilité de l'accident, s'était retrouvé dans ses dossiers. Les policiers qui avaient fait le constat de l'accident avaient jugé que le conducteur de l'autre véhicule était responsable.

La Direction générale a constaté que le rapport en question s'inscrivait dans le contexte d'une étude en cours sur les accidents mortels de la route réalisée par des universités locales pour le compte de Transports Canada. L'étude avait pour but l'analyse des accidents afin qu'on puisse en déterminer les raisons et mesurer l'efficacité d'un certain nombre de nouveaux dispositifs de sécurité dont les véhicules doivent désormais être équipés. Les rapports en question n'ont jamais été conçus pour remplacer ou compléter les enquêtes policières locales.

Avant 1978, les rapports préparés étaient longs et contenaient beaucoup de renseignements personnels que des gens bien informés auraient pu relier à un accident donné. Ils étaient conservés ouvertement dans des bibliothèques gouvernementales. Dans ce cas-ci, il semble qu'un agent de police local qui aurait été apparenté aux victimes aurait remis le rapport à la Société d'assurance.

Bien que l'incident se soit produit avant l'entrée en vigueur de la Loi, il a fait prendre conscience au Commissariat que ces rapports étaient disponibles et qu'on s'en servait. L'enquête a révélé que la formule de rapport présentement utilisée est plus courte, qu'il n'y figure plus que quelques renseignements personnels, et que les rapports sont transférés électroniquement aux dossiers nationaux des accidents.

Le Commissariat a étudié les méthodes de conservation des vieux rapports et des nouveaux et il a formulé un certain nombre de recommandations pour protéger la vie privée des victimes et des responsables des accidents. Transports Canada a volontiers accepté de mettre en oeuvre de nouveaux mécanismes limitant l'accès aux données et a garanti qu'elles ne seraient désormais plus utilisées que pour la recherche.

La Loi sur les marques de commerce prévaut

Un enquêteur du Commissariat s'est fait dire au cours d'une conversation téléphonique qu'environ 20 000 dossiers «protégés» (la désignation de sécurité correspondant aux renseignements personnels) étaient conservés dans un bureau ouvert situé dans un hall public d'un immeuble gouvernemental de Hull.

Quand les enquêteurs ont visité les lieux, qui abritent le Bureau de l'enregistrement des marques de commerce de Consommation et Corporations Canada (CCC), ils y ont trouvé les noms et adresses des personnes qui avaient demandé une marque de commerce enregistrée. Or la *Loi sur la protection des renseignements personnels* exige que ces renseignements soient protégés.

Les autorités du Ministère ont toutefois fait valoir que la *Loi sur les marques de commerce* est claire : ces renseignements doivent être à la disposition du public pour inspection. Étant donné que la *Loi sur la protection des renseignements personnels* protège ces renseignements contre toute communication à des tiers «sous réserve d'autres lois du Parlement», il en résulte que la conservation de ces dossiers dans un endroit complètement accessible au public ne constitue pas une infraction. Néanmoins, les enquêteurs ont constaté l'existence de problèmes mineurs de sécurité physique et ils les ont signalés aux responsables ministériels de la protection de la vie privée, qui s'occupent de les régler.

GESTION INTÉGRÉE

La Gestion intégrée fournit des services en matière de finances, de personnel, d'administration, d'informatique et de bibliothèque au Commissariat à l'information et au Commissariat à la protection de la vie privée.

Finances

Un nouveau système de contrôle budgétaire informatisé a été mis en place afin d'améliorer le suivi et les rapports relatifs aux engagements financiers et aux dépenses.

Ci-dessous les dépenses des commissariats pour la période allant du 1er avril 1989 au 31 mars 1990*

	Information	Vie Privée	Gestion intégrée	Total
Salaires	1,585,156	1,794,669	505,526	3,885,351
Contributions aux régimes d'avantages sociaux des employés	243,000	274,000	79,000	596,000
Transports et communications	36,925	86,040	130,663	253,628
Information	25,133	36,699	2,394	64,226
Services professionnels et spéciaux	595,374	68,916	51,493	715,783
Location	—	2,381	10,588	12,969
Achats de services de réparation et d'entretien	2,185	14,271	4,256	20,712
Services publics, fournitures et approvisionnements	16,064	14,330	37,974	68,368
Acquisition de machines et d'équipement	31,562	38,933	62,031	132,526
Autres dépenses	1,474	3,521	2,711	7,706
TOTAL	**2,536,873**	**2,333,760**	**886,636**	**5,757,269**

*Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des comptes publics 1989-1990 traitant des Commissariats.

Le budget des commissariats pour l'année financière 1989-1990 s'élevait à 5 856 000 $ et à 75 années-personnes, soit une augmentation de 765 000 $ et de 6 années-personnes par rapport à 1988-1989. Les dépenses engagées au titre du personnel (4 481 351 $) et des services professionnels et spéciaux (715 783 $) ont représenté plus de 90 pour 100 des fonds décaissés. Le reste, soit (560 135 $) a servi à couvrir les autres dépenses.

Personnel

Avec une augmentation nette de six années-personnes, la nomination pour la première fois d'un Commissaire adjoint à la protection de la vie privée et la venue à terme du mandat d'un Commissaire adjoint à l'information, le programme du personnel a été fort occupé, encore une fois, au cours de 1989-1990. En effet, ce service a procédé à 38 opérations de dotation, y compris celle d'un poste de haute gestion, ainsi qu'à une revue de tous les postes du groupe de l'administration des programmes (PM) rendue nécessaire par l'entrée en vigueur des nouvelles normes de classification. Les commissariats ont également fait l'objet d'une vérification des opérations de dotation par la Commission de la fonction publique.

Administration

Comme conséquence de la croissance de notre organisme et pour répondre aux besoins futurs, nous avons obtenu de nouveaux locaux.

Informatique

Le Commissariat à la protection de la vie privée s'est doté d'un réseau local qui lui permettra d'augmenter sa production de rapports et de documents.

Des travaux préliminaires ont également été entrepris pour tenir compte des changements majeurs au système de gestion des cas, maintenant désuet. Une étude des besoins du système de gestion des cas du Commissariat à l'information a été entreprise.

Les Commissariats ont aussi commencé une nouvelle infrastructure de gestion informatisée, pour répondre à leurs besoins croissants.

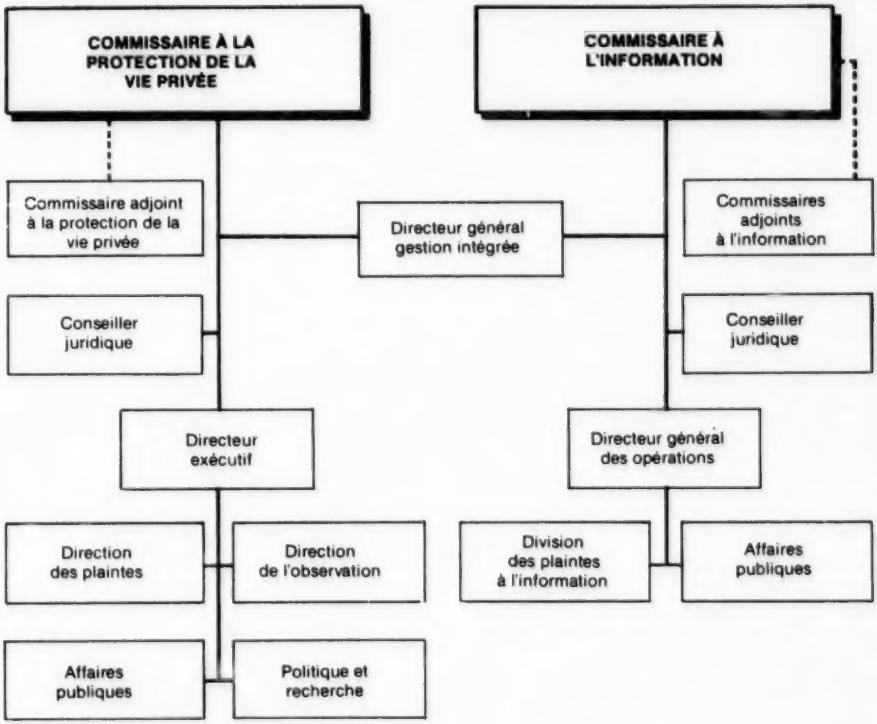
Bibliothèque

La bibliothèque dessert les programmes du Commissariat à la protection de la vie privée et du Commissariat à l'information. Le public y a accès pour fins de consultation.

Parmi les services qu'elle offre, citons les prêts inter-bibliothèques, la documentation et la recherche manuelles et automatisées et la tenue de dossiers thématiques de coupures de presse. La bibliothèque acquiert et conserve des documents canadiens et étrangers sur tous les aspects de la liberté d'accès à l'information, du droit à la vie privée, de la protection des données et de la fonction de protecteur du citoyen. Elle tient également des collections importantes de rapports annuels sur l'administration des lois et de rapports annuels des ombudsmen.

L'informatisation des fonctions de la bibliothèque est en cours. Le cataloguage interne en direct de notre collection nous permet de produire rapidement et efficacement des bibliographies thématiques, des listes des périodiques reçus et des statistiques sur la diffusion de documents.

Annexe I


COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE
COMMISSAIRE À L'INFORMATION
Commissaire adjoint à la protection de la vie privée
Directeur général gestion intégrée
Commissaires adjoints à l'information
Conseiller juridique
Conseiller juridique
Directeur exécutif
Directeur général des opérations
Direction des plaintes
Direction de l'observation
Division des plaintes à l'information
Affaires publiques
Affaires publiques
Politique et recherche

Annexe II

Institutions fédérales assujetties à la Loi

Administrateur de l'Office du transport du grain

Administration de la voie maritime du Saint-Laurent

Administration de pilotage de l'Atlantique

Administration de pilotage des Grands Lacs, Limitée

Administration de pilotage des Laurentides

Administration de pilotage du Pacifique

Administration du pipe-line du Nord

Administration du rétablissement agricole des Prairies

Affaires des anciens combattants Canada

Affaires extérieures Canada

Affaires indiennes et du Nord Canada

Agence canadienne de développement international

Agence de promotion économique du Canada Atlantique

Agence de surveillance du secteur pétrolier

Agriculture Canada

Approvisionnements et Services Canada

Archives nationales du Canada

Banque du Canada

Banque fédérale de développement

Bibliothèque nationale

Bourse fédérale d'hypothèques

Bureau canadien de la sécurité aérienne

Bureau de l'enquêteur correctionnel

Bureau de l'inspecteur général du service canadien du renseignement de sécurité

Bureau du Conseil privé

Bureau du contrôleur général

Bureau de la coordonnatrice de la situation de la femme

Bureau du directeur des enquêtes et recherches

Bureau du Directeur général des élections

Bureau du séquestre (biens ennemis)

Bureau de services juridiques des pensions

Bureau du Surintendant des institutions financières Canada

Bureau du vérificateur général

Centre canadien d'hygiène et de sécurité au travail

Centre de recherche pour le développement international

Centre national des Arts, Corporation du

Comité externe d'examen de la Gendarmerie royale du Canada

Comité de surveillance des activités de renseignement de sécurité

Commissariat aux langues officielles

Commission d'appel des pensions

Commission canadienne des droits de la personne

Commission canadienne d'examen des exportations des biens culturels

Commission canadienne des grains

Commission canadienne du blé

Commission canadienne du lait

Commission de la Capitale nationale

Commission canadienne des pensions

Commission des champs de bataille nationaux

Commission de contrôle de l'énergie atomique

Commission de l'emploi et de l'immigration du Canada

Commission d'énergie du Nord canadien

Commission de la Fonction publique

Commission de l'immigration et du statut de réfugié

Commission d'indemnisation des marins marchands

Commission des lieux et monuments historiques du Canada

Commission nationale des libérations conditionnelles

Commission des plaintes du public contre la Gendarmerie royale du Canada

Commission de réforme du droit du Canada

Commission des relations de travail dans la Fonction publique

Commission de révision des lois

Communications, Ministère des

Conseil des Arts du Canada

Conseil canadien des normes

Conseil canadien des relations de travail

Conseil consultatif de recherches sur les pêcheries et les océans

Conseil consultatif de la situation de la femme

Conseil de contrôle des renseignements relatifs aux matières dangereuses

Conseil économique du Canada

Conseil de fiducie du Fonds canadien de recherches de la Reine Élisabeth II sur les maladies de l'enfance

Conseil national de commercialisation des produits de ferme

Conseil national de l'esthétique industrielle

Conseil national de recherches du Canada

Conseil de la radiodiffusion et des télécommunications canadiennes

Conseil de recherches médicales

Conseil de recherches en sciences humaines

Conseil de recherches en sciences naturelles et en génie

Conseil des Sciences du Canada

Conseil des subventions au développement régional

Conseil du Trésor, Secrétariat du

Consommation et Corporations Canada

Construction de défense (1951) Limitée

Corporation commerciale canadienne

La Corporation du Pont international de la voie maritime, Ltée

Défense nationale

Directeur de l'établissement de soldats

Directeur des terres destinées aux anciens combattants

Emploi et Immigration Canada

Énergie, Mines et Ressources Canada

Environnement Canada

Finances, Ministère des

Gendarmerie royale du Canada

Industrie, Sciences et Technologie

Institut canadien pour la paix et la sécurité internationale

Investissement Canada

Justice Canada, Ministère de la

Monnaie royale canadienne

Musée des Beaux-Arts du Canada

Musée canadien des civilisations

Musée canadien de la guerre

Musée national de l'aviation

Musée national des sciences naturelles

Musée national de la poste

Musée national des sciences et de la technologie

Office Canada-Nouvelle-Écosse des hydrocarbures extra-côtiers

Office Canada-Terre-Neuve des hydrocarbures extra-côtiers

Office canadien du poisson salé

Office canadien des provendes

Office de commercialisation du poisson d'eau douce

Office des eaux des territoires du Nord-Ouest

Office des eaux du territoire du Yukon

Office des indemnisations pétrolières

Office national de l'énergie

Office national du film

Office national des transports (auparavant la Commission canadienne des transports)

Office des normes du gouvernement canadien

Office des prix des produits de la pêche

Office des produits agricoles

Office de répartition des approvisionnements d'énergie

Office de stabilisation des prix agricoles

Pêches et Océans Canada

Les Ponts Jacques-Cartier et Champlain Incorporée

Privatisation et affaires réglementaires

Revenu Canada

Santé et Bien-être social Canada

Secrétariat des relations fédérales-provinciales

Secrétariat d'État

Service canadien du renseignement de sécurité

Service correctionnel Canada

Service national des libérations conditionnelles

Société canadienne des brevets et d'exploitation Ltée

Société canadienne d'hypothèque et de logement

Société canadienne des ports

Société canadienne des postes

Société d'assurance-dépôt du Canada

Société de développement de l'industrie cinématrographie y inclus Téléfilm Canada

Société du crédit agricole

Société immobilière du Canada Limitée

Société pour l'expansion des exportations

Solliciteur général Canada

Statistique Canada

Transports Canada

Travail Canada

Travaux publics Canada

Tribunal d'appel des anciens combattants

Tribunal canadien du commerce extérieur